Welcome To

ISSCC 2014
SESSION 16

SoC Building Blocks

A 340mV-to-0.9V 20.2Tb/s Source-Synchronous Hybrid Packet/Circuit-Switched 16x16 Network-on-Chip in 22nm Tri-Gate CMOS

Gregory Chen, Mark A Anders, Himanshu Kaul, Sudhir K Satpathy, Sanu K Mathew, Steven K Hsu, Amit Agarwal, Ram K Krishnamurthy, Shekhar Borkar, Vivek De

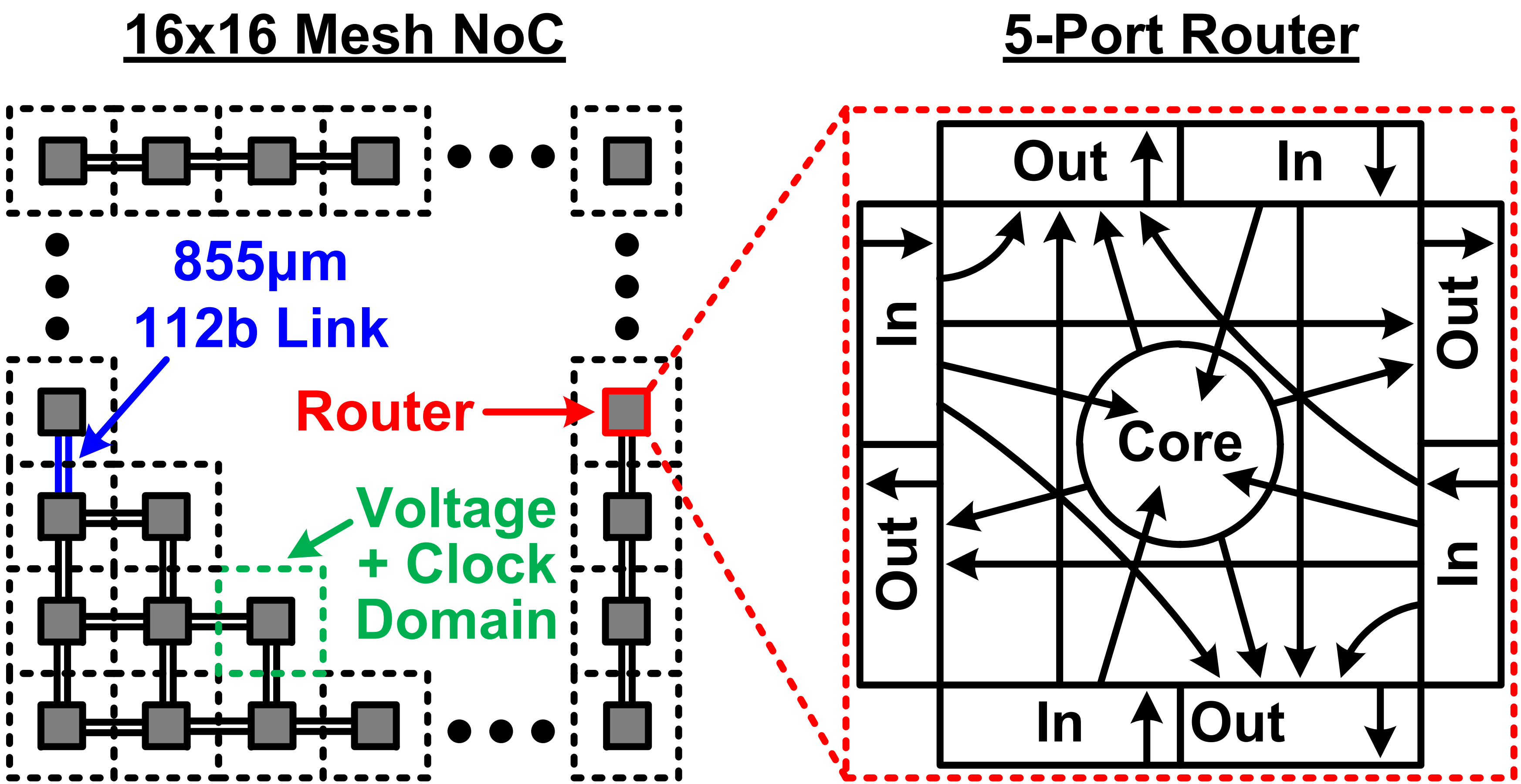
Circuits Research Lab, Intel Corporation

This research was, in part, funded by the U.S. Government under contract number HR0011-10-3-0007. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government.

Outline

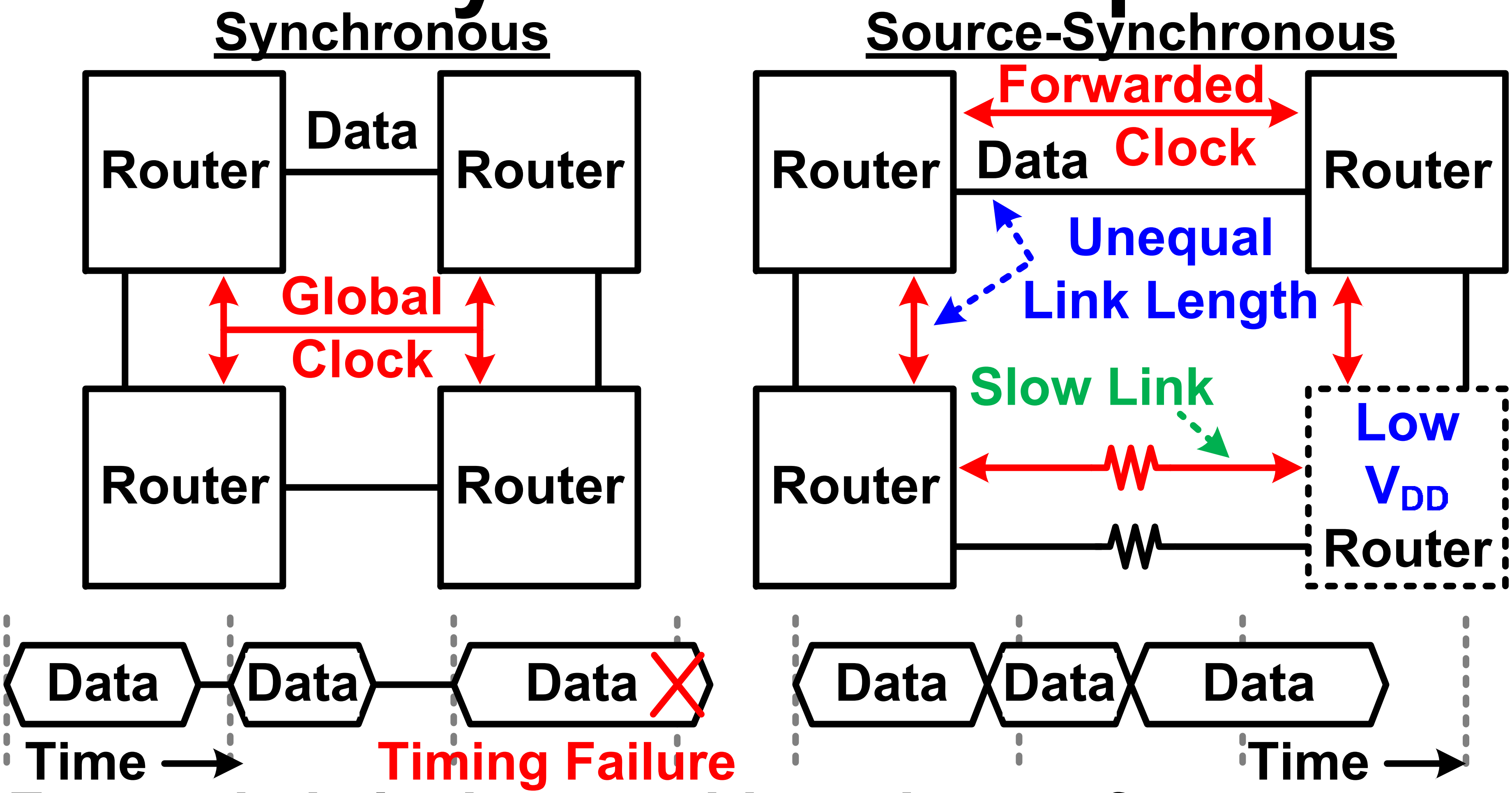
- 16x16 Network-on-Chip (NoC) organization
- Packet credit tracking and direction arbitration
- Channel reservation circuits
- Data transfer and acknowledgement circuits
- Measurement results in 22nm tri-gate CMOS
- Summary

16x16 NoC Organization



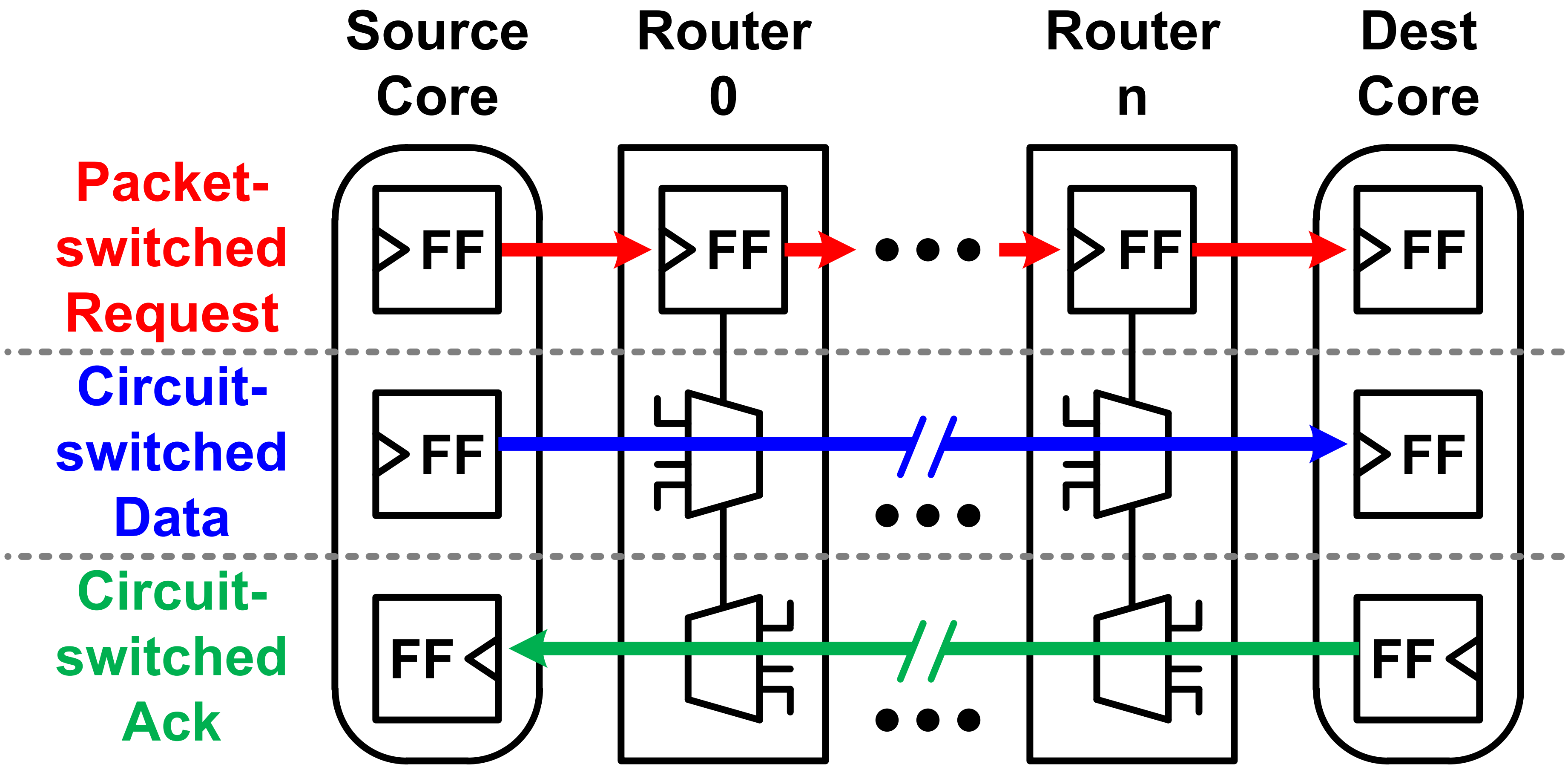
- On-chip communication is a performance/power limiter for future exa-scale multi-core processors
- Support design heterogeneity and delay variations

Source-Synchronous Operation



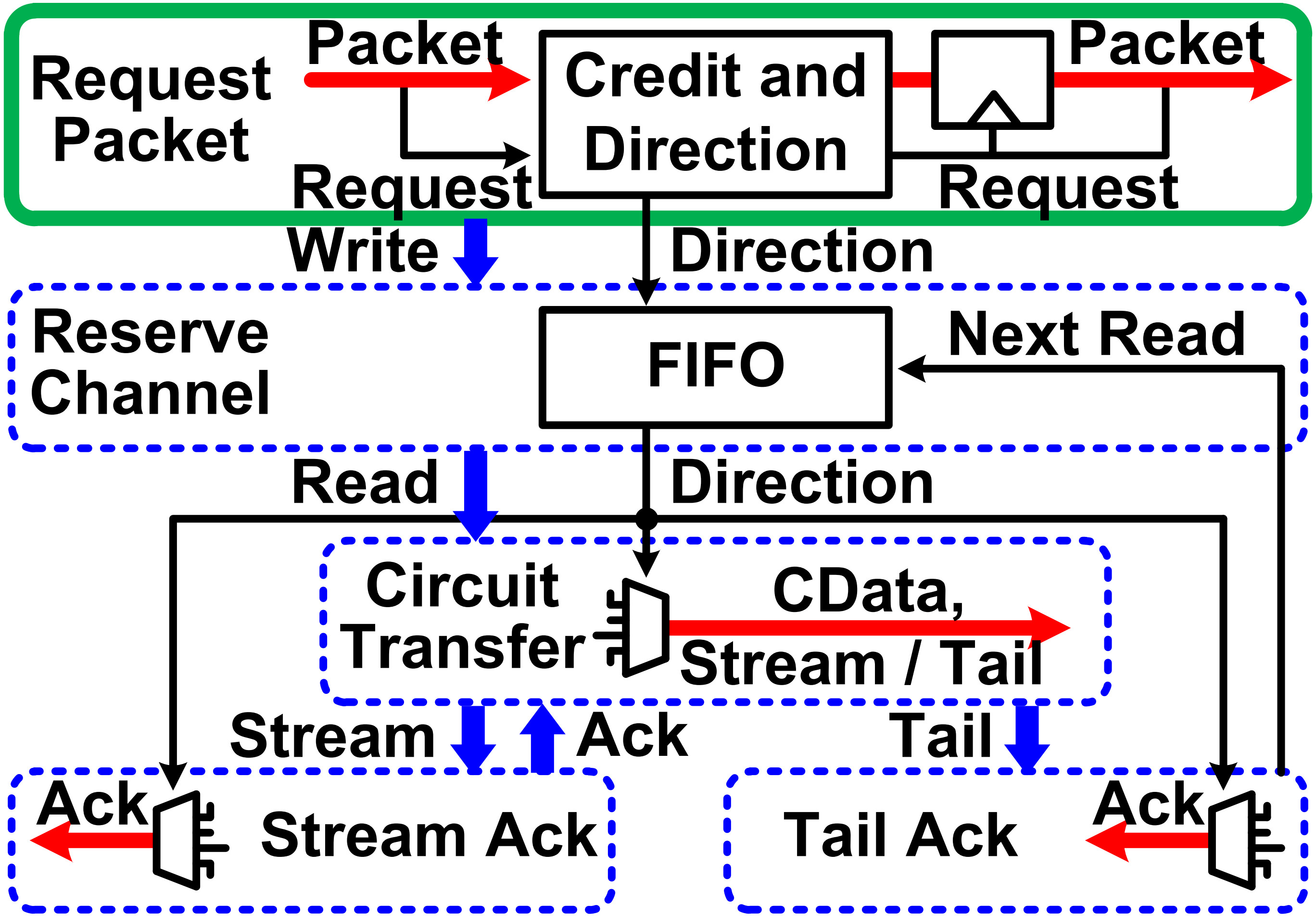
- Forwarded clock sent with each transfer
- Delay-adaptive for multiple voltage/clock domains
- Delay averaging for resilience to process variation

Hybrid Packet/Circuit Switching



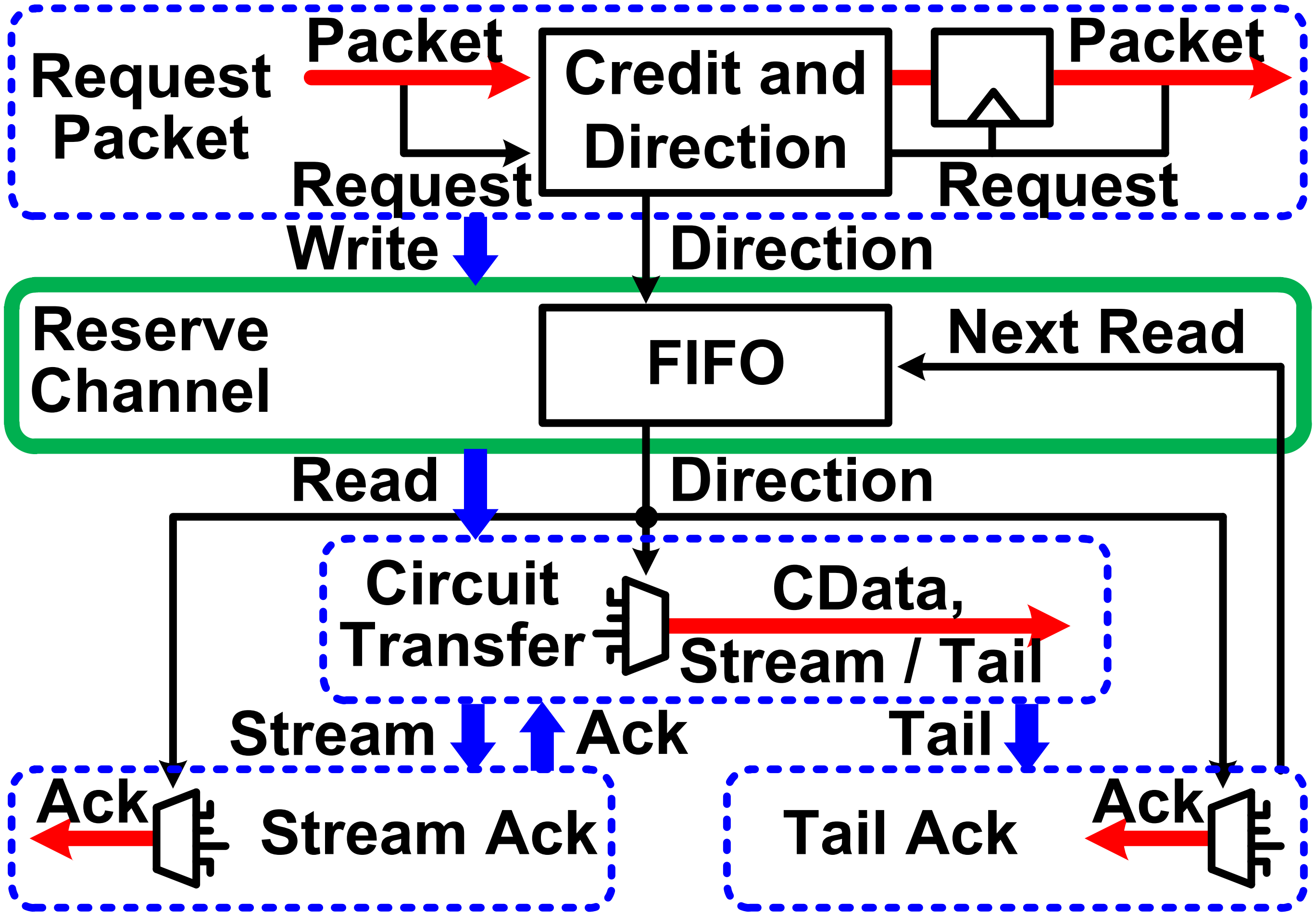
- Packet-switched requests reserve circuit channels
- Circuit-switched data with no intra-route storage
- Ack indicates completed transfer

NoC Operation



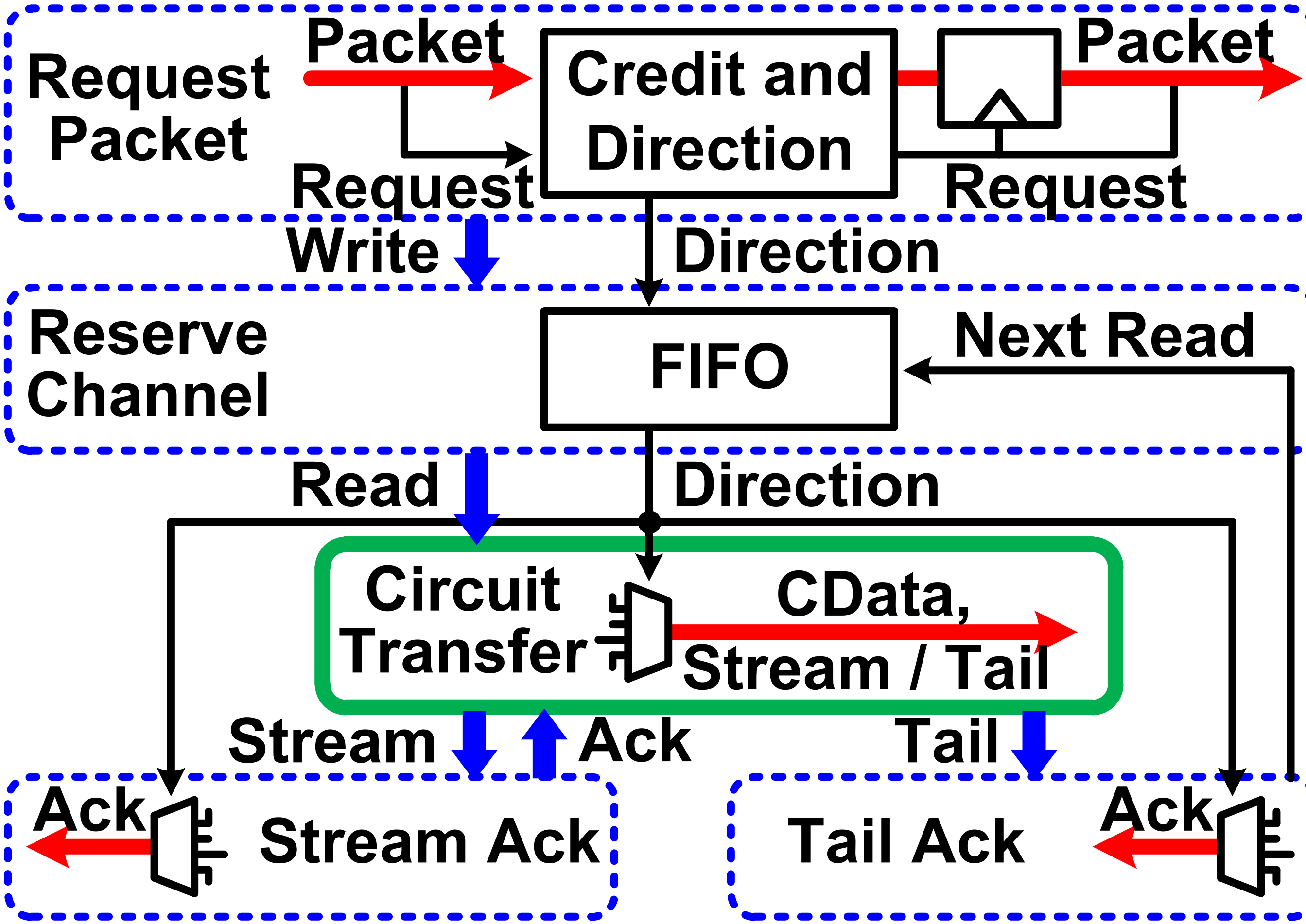
- Request packet with single pipeline stage per router
- Credit tracking controls the request packet pipeline

NoC Operation



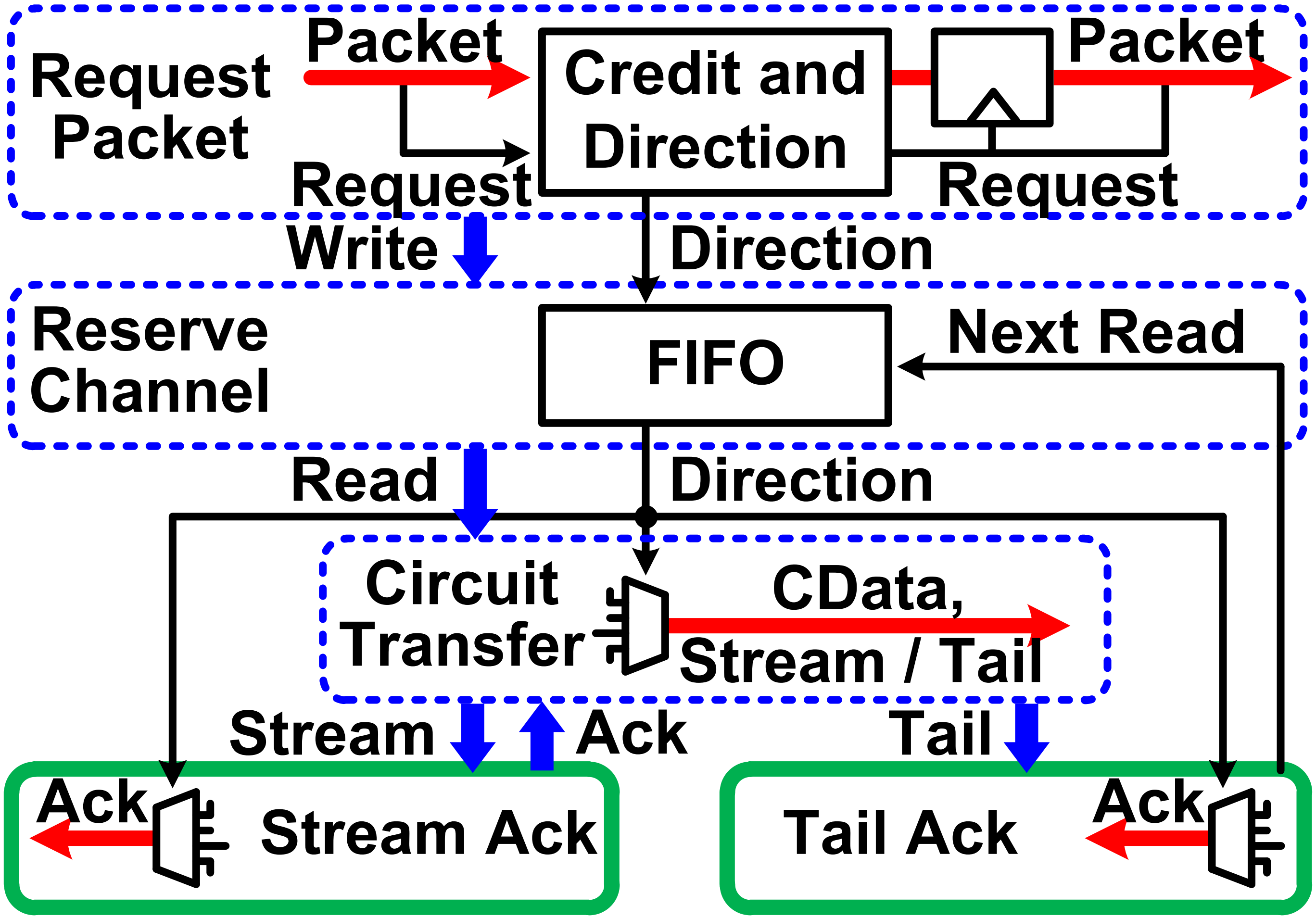
- FIFO queues channel setup direction
- Request packets propagate ahead of circuit transfer

NoC Operation



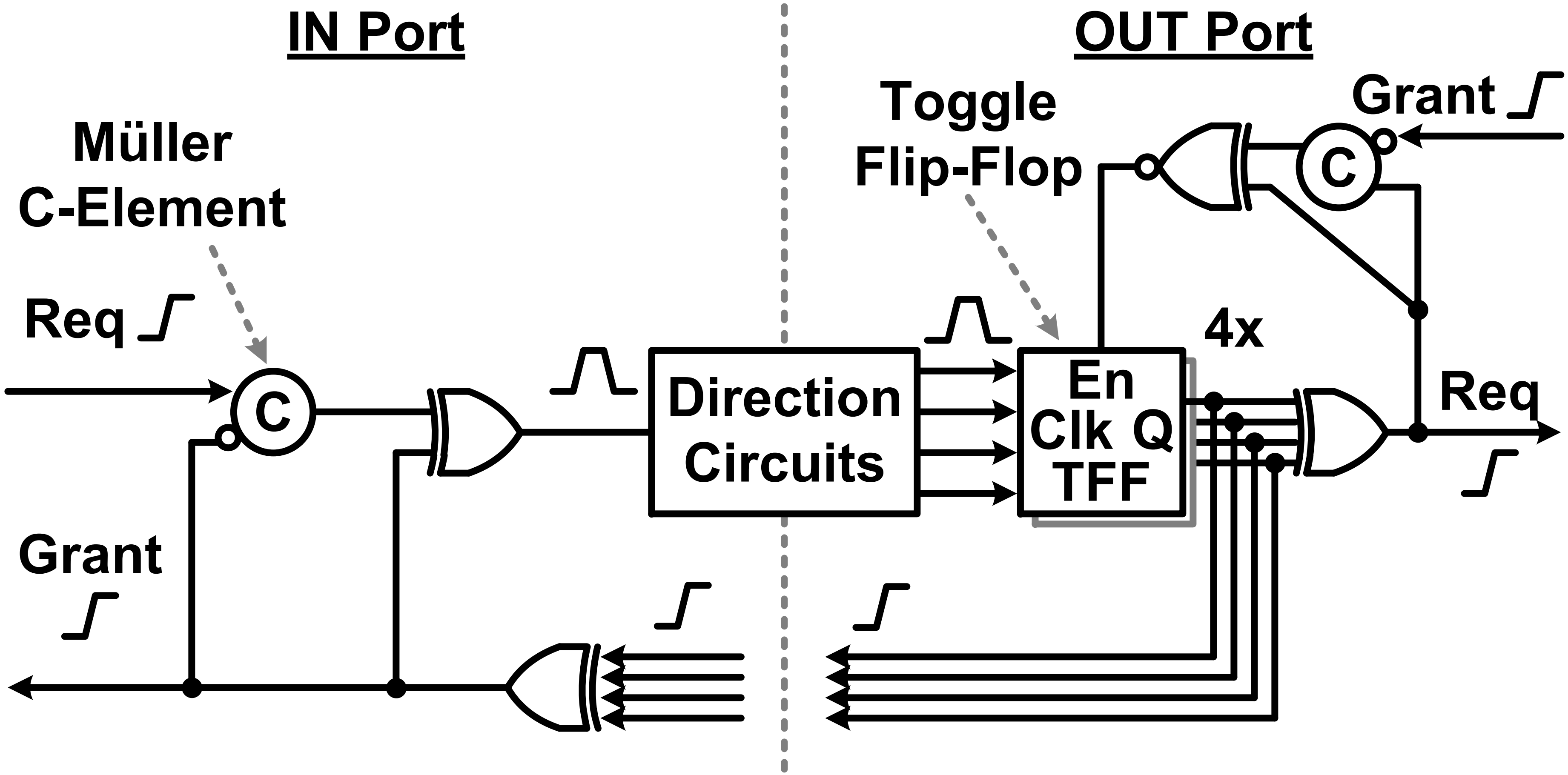
- Direction configures circuit-switched channel
- Circuit transfer occurs without intra-route storage

NoC Operation



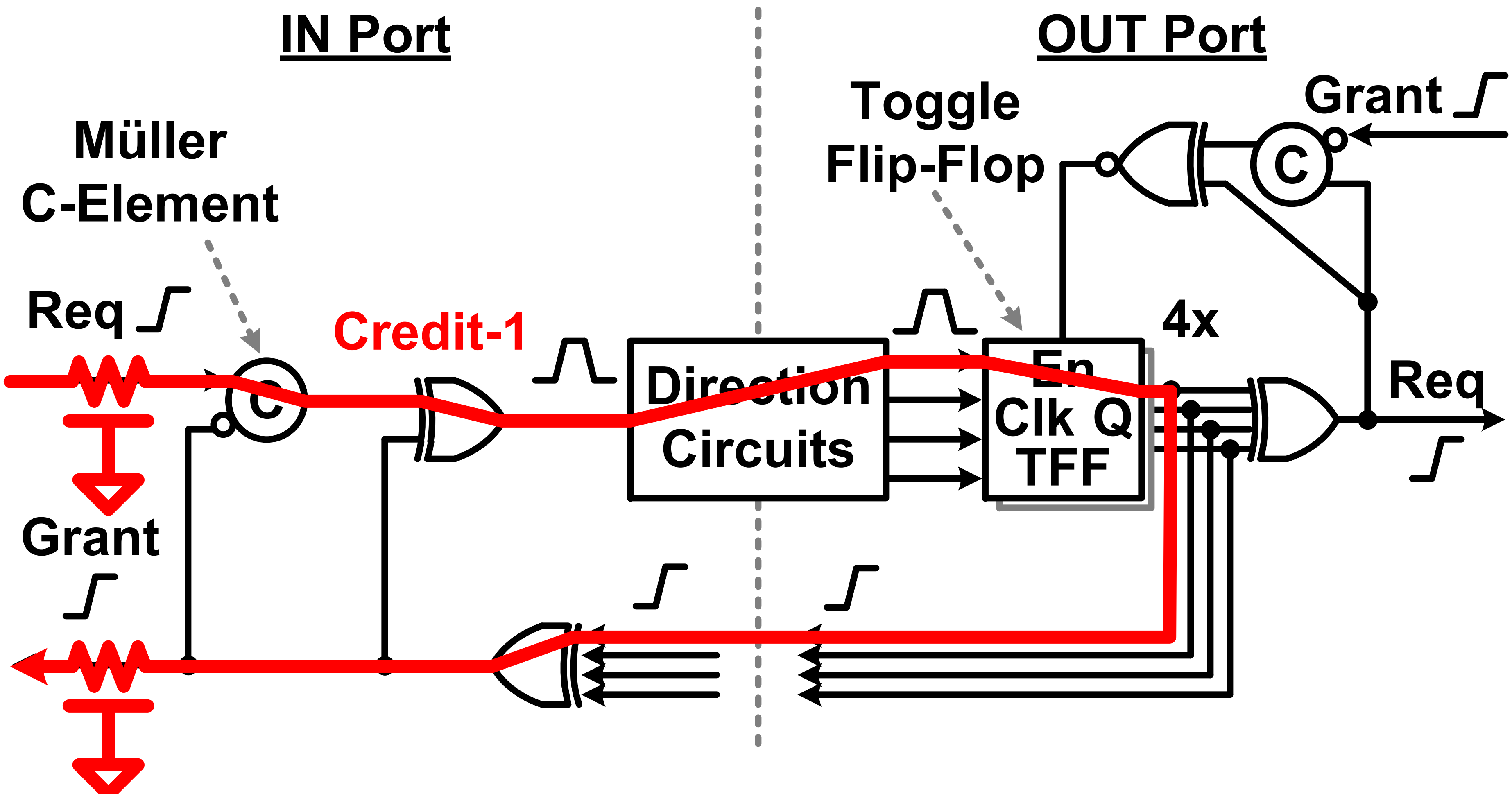
- Streaming amortizes channel setup energy
- Tail Ack deallocates circuit-switched channel

Credit Tracking Circuits



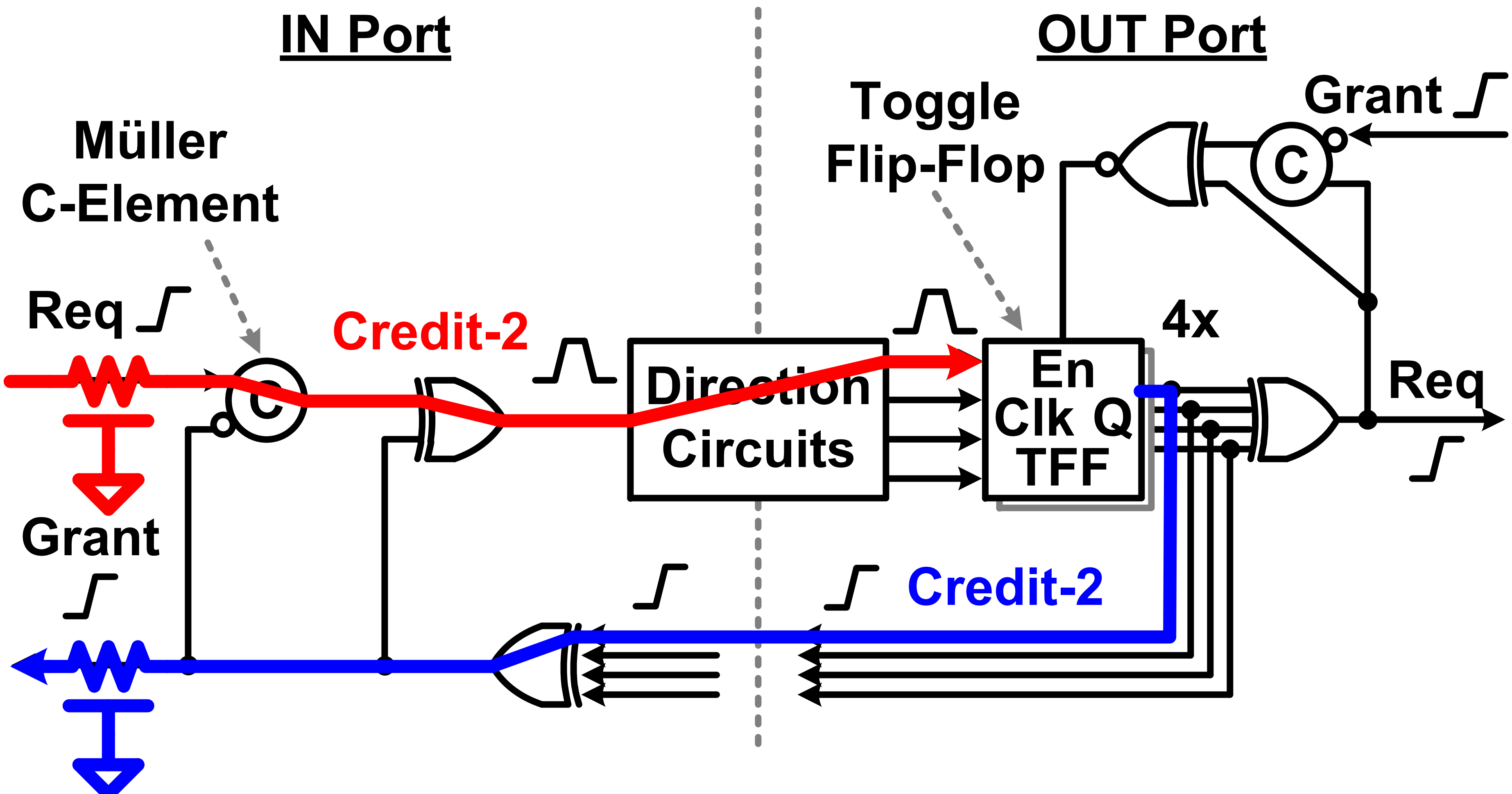
- Credit-2 removes round-trip latency between routers
- Improves packet throughput by 89%

Credit Tracking Circuits



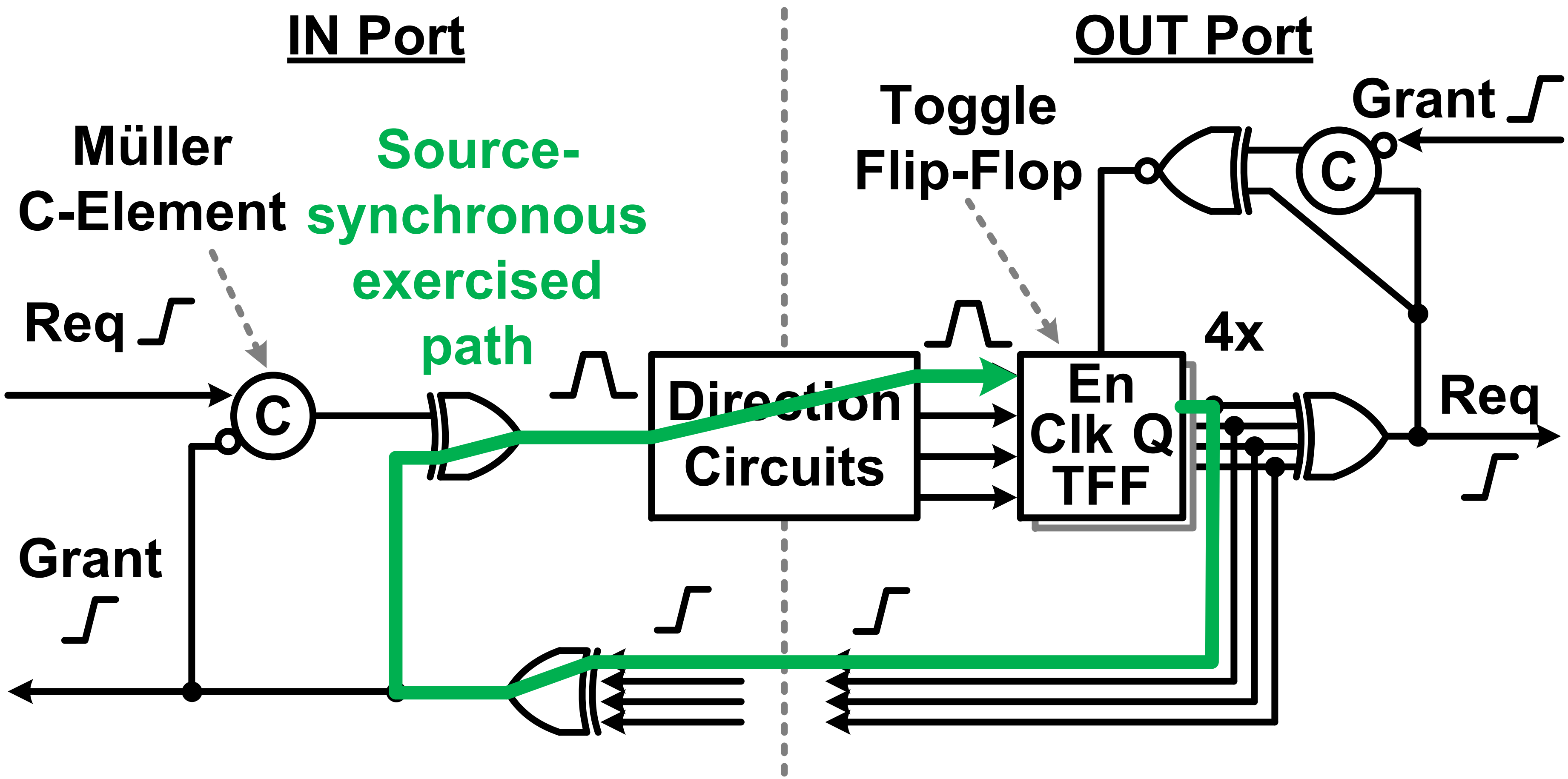
- Credit-2 removes round-trip latency between routers
- Improves packet throughput by 89%

Credit Tracking Circuits



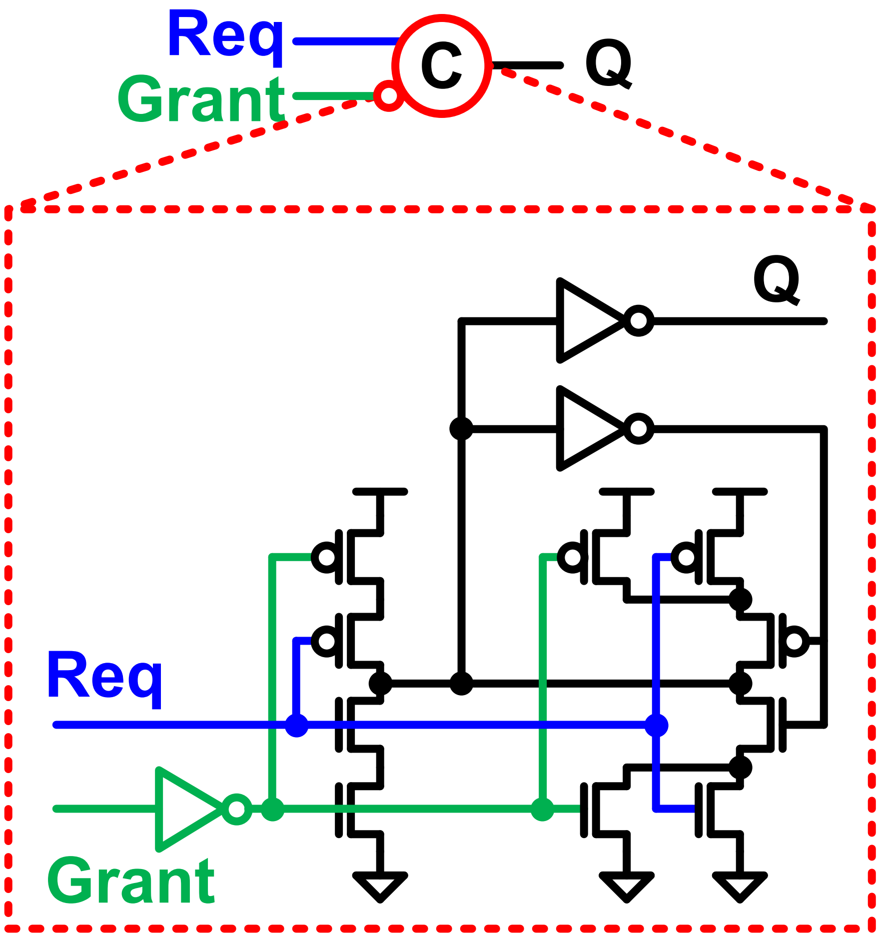
- Credit-2 removes round-trip latency between routers
- Improves packet throughput by 89%

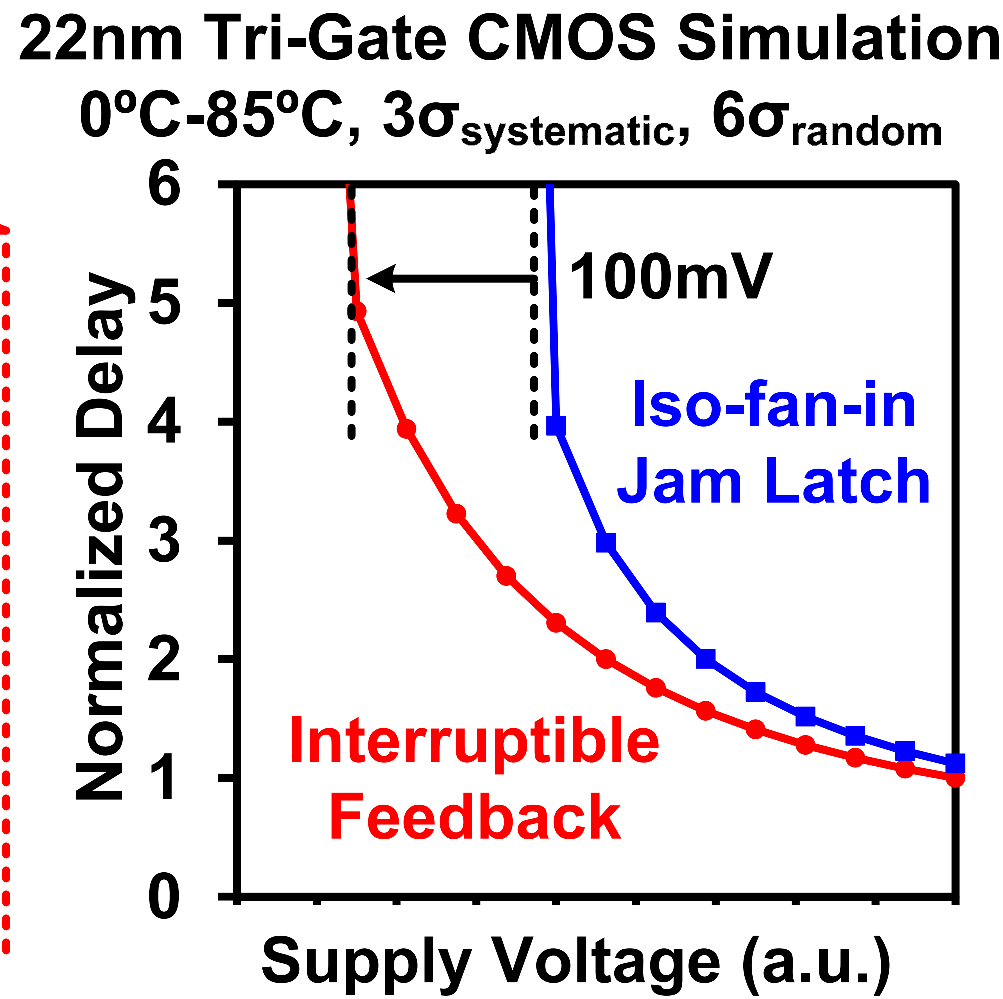
Credit Tracking Circuits



- Latency set by exercised instead of worst-case path
- Improves packet throughput by 35%

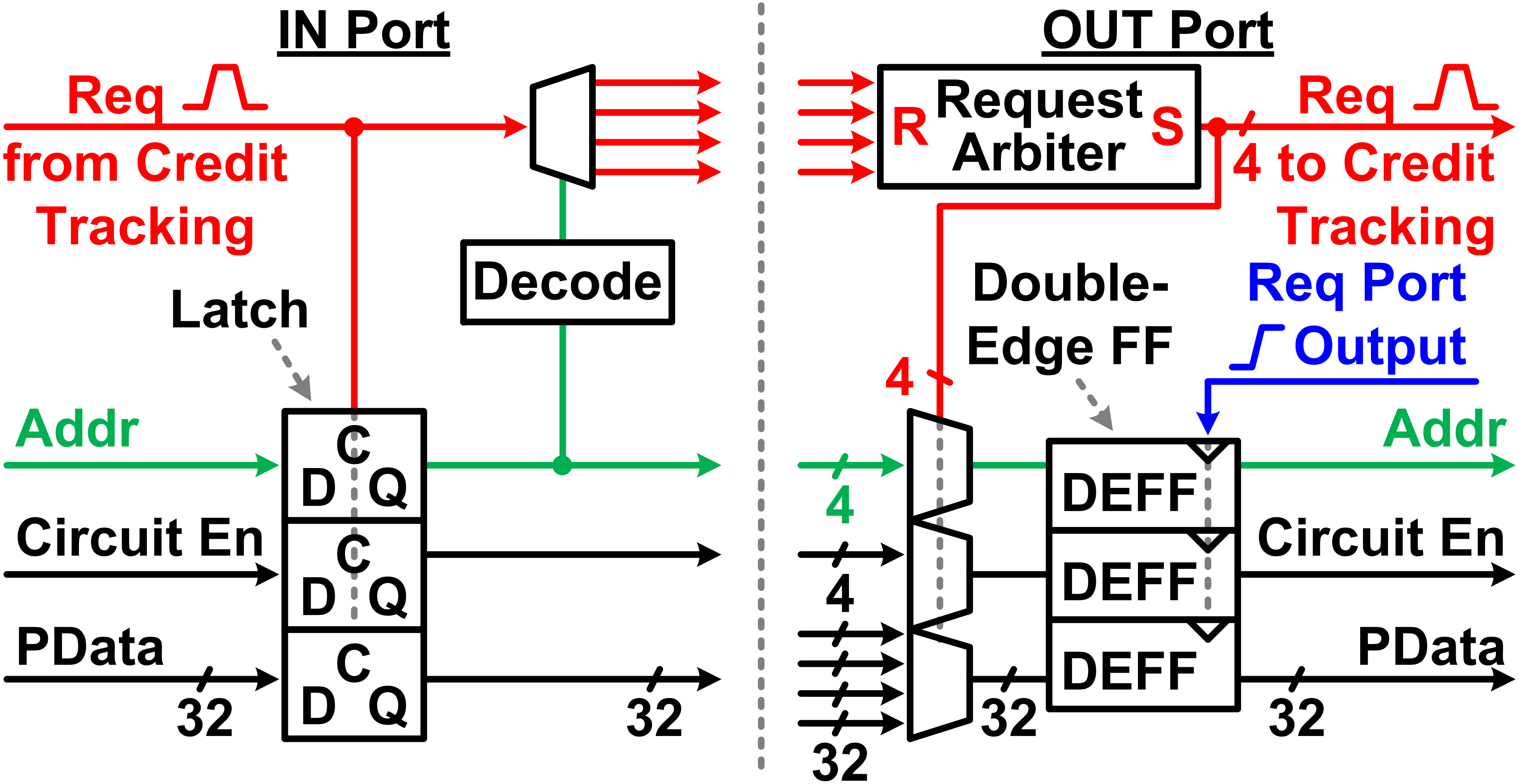
Credit Tracking C-Element





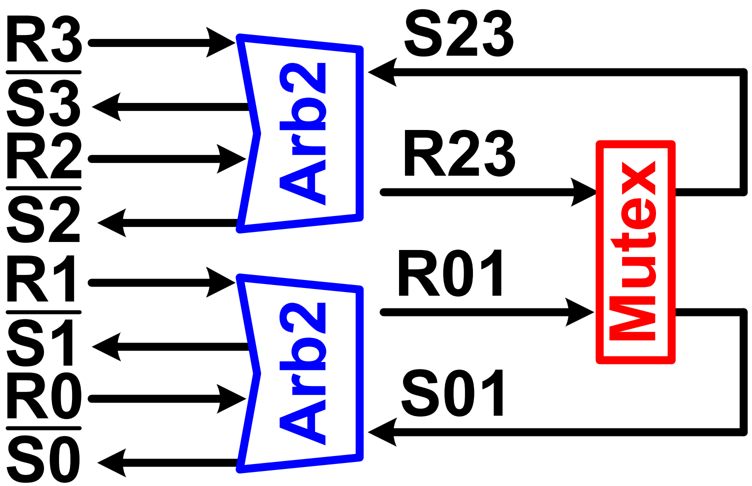
- Single C-element in IN and OUT Ports tracks credit
- Interruptible feedback lowers V_{MIN} by 100mV

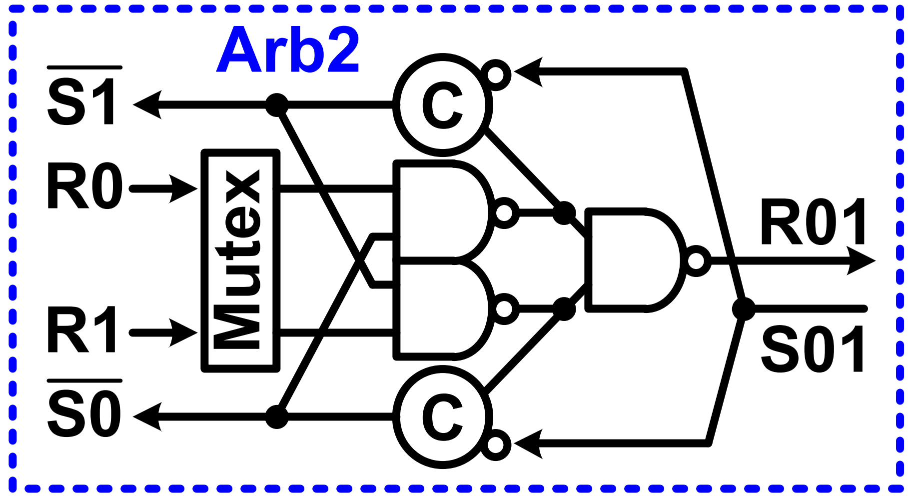
Packet Direction Circuits

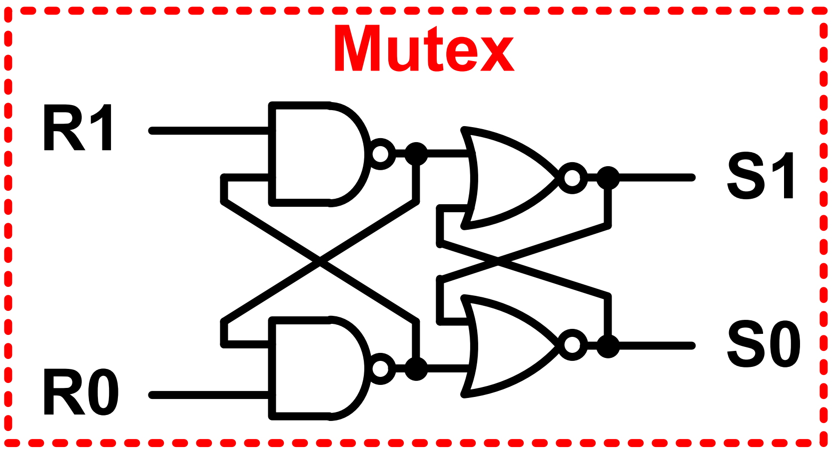


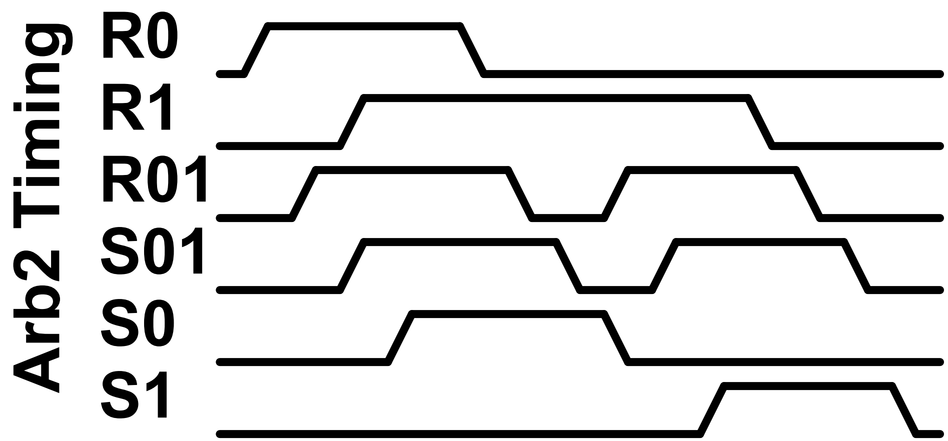
- 32b sideband improves throughput by 72%
- Input latches block packet when router is busy
- Double-edge flip-flop reduces clock power by 25%

Request Arbiter



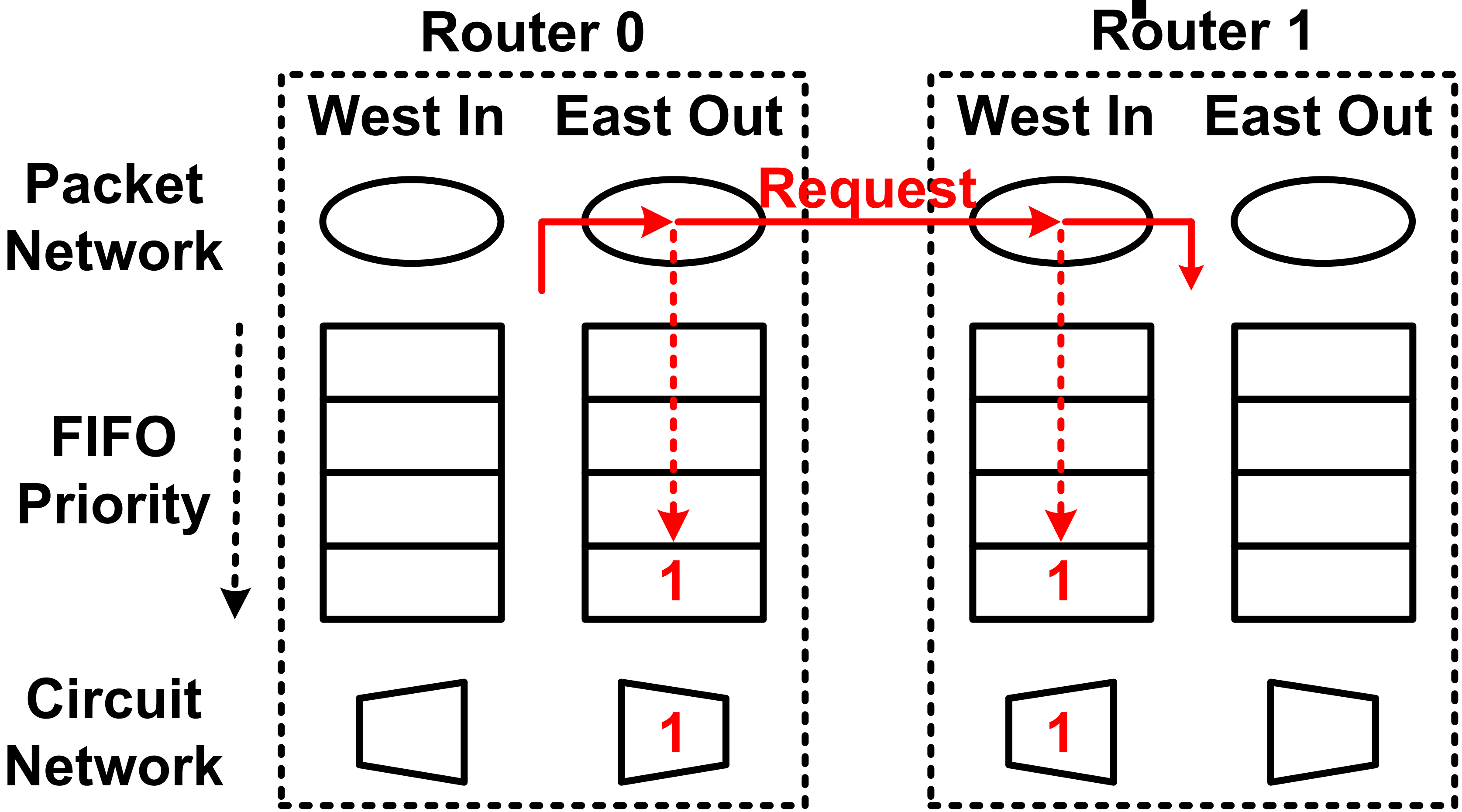






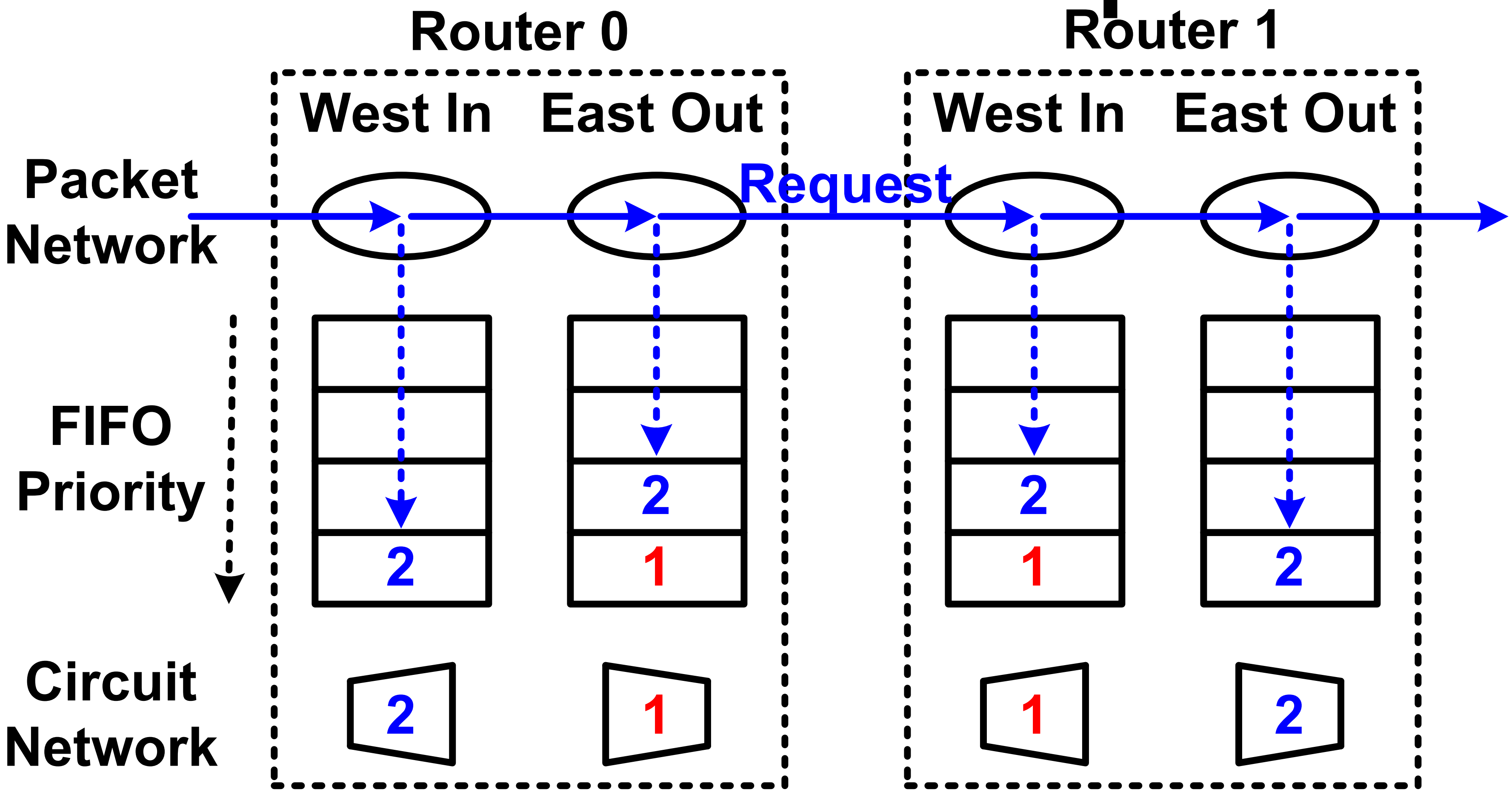
- Coordinates requests from multiple IN Ports
- Optimized 2nd-level mutex for 33% reduced latency

Channel Reservation Operation



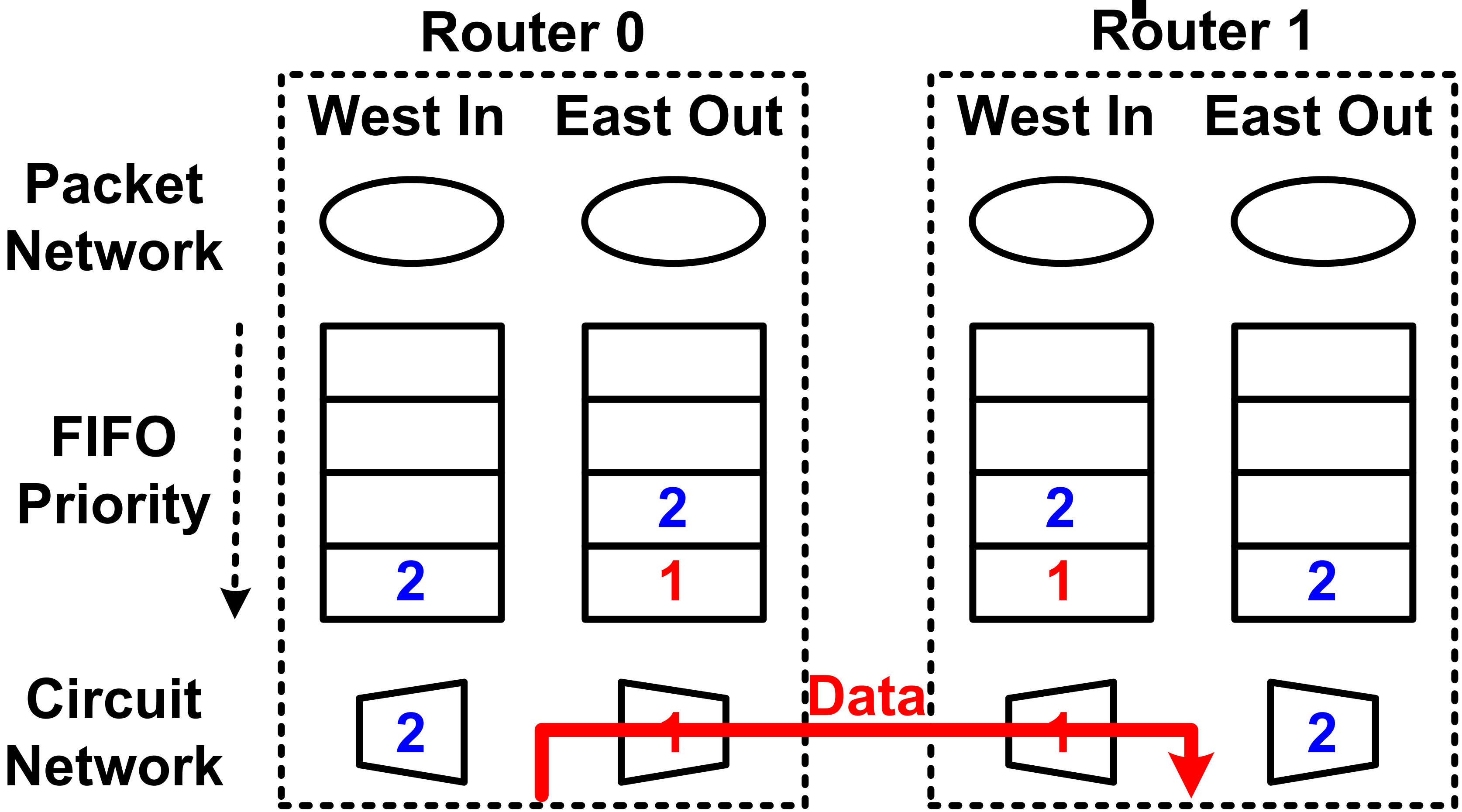
- Packets store direction for later channel setup
- Requests cleared after circuit transfer completion
- Hides request packet delay for 62% lower latency

Channel Reservation Operation



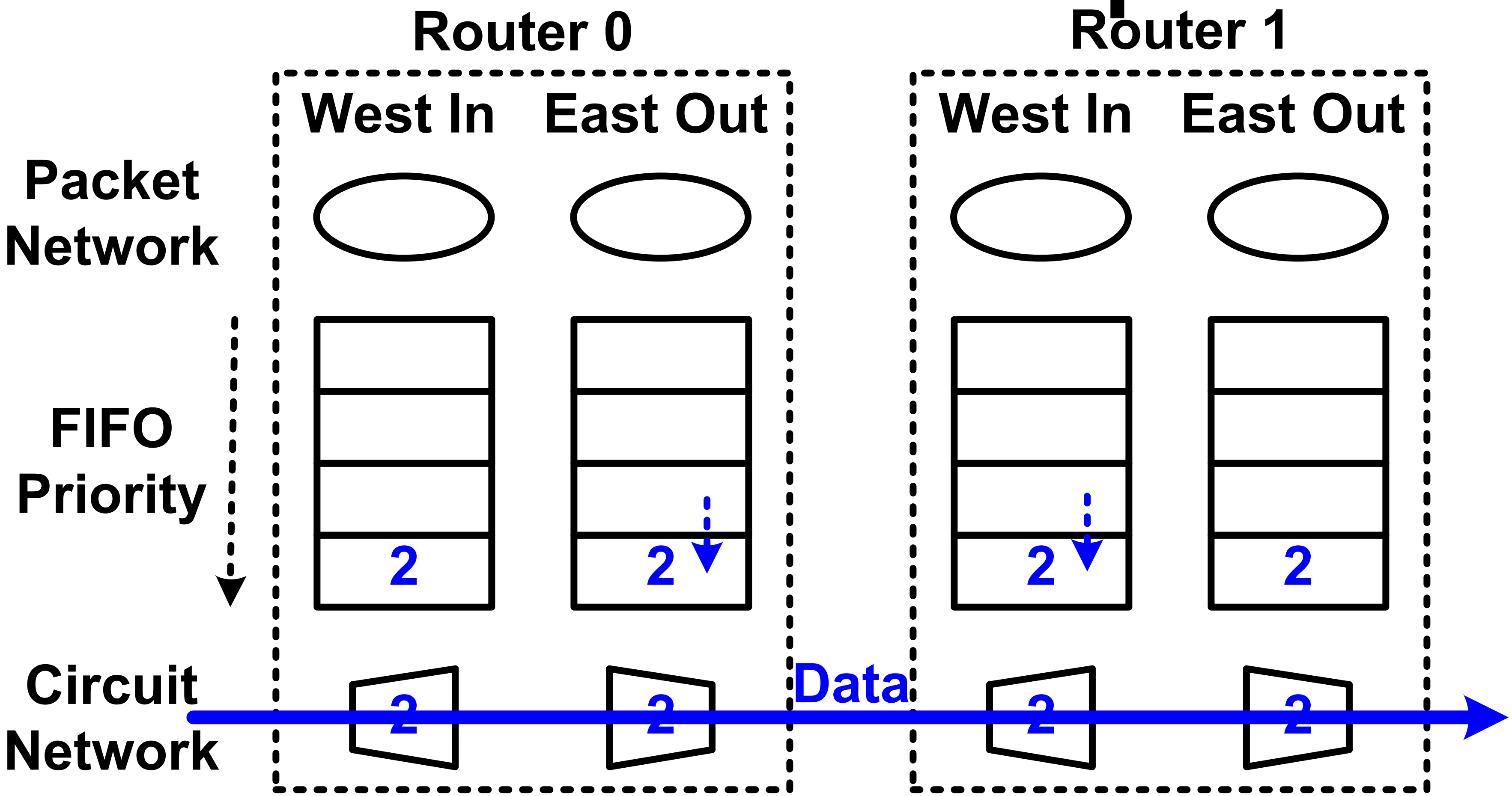
- Packets store direction for later channel setup
- Requests cleared after circuit transfer completion
- Hides request packet delay for 62% lower latency

Channel Reservation Operation



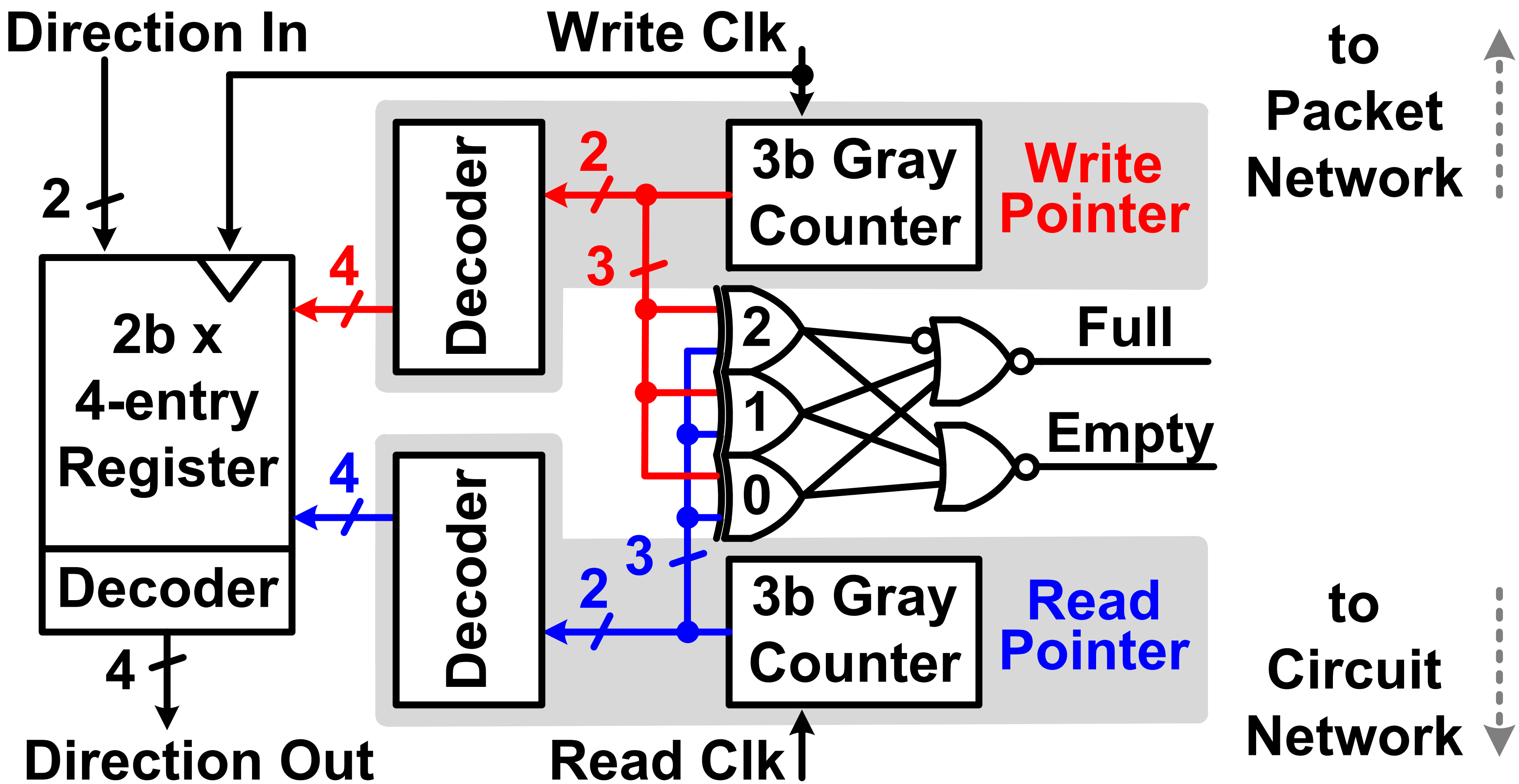
- Packets store direction for later channel setup
- Requests cleared after circuit transfer completion
- Hides request packet delay for 62% lower latency

Channel Reservation Operation



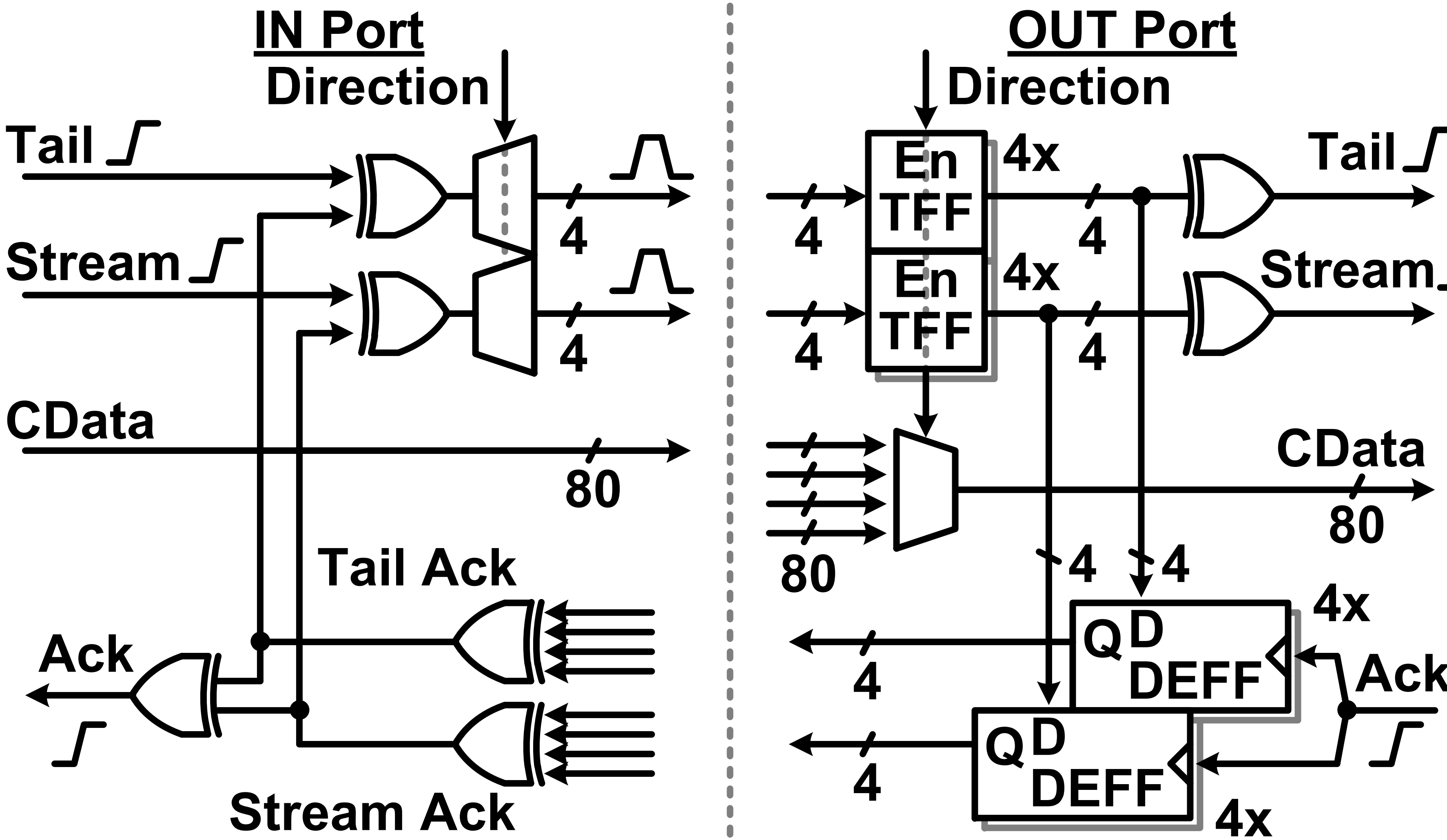
- Packets store direction for later channel setup
- Requests cleared after circuit transfer completion
- Hides request packet delay for 62% lower latency

Channel Reservation FIFO



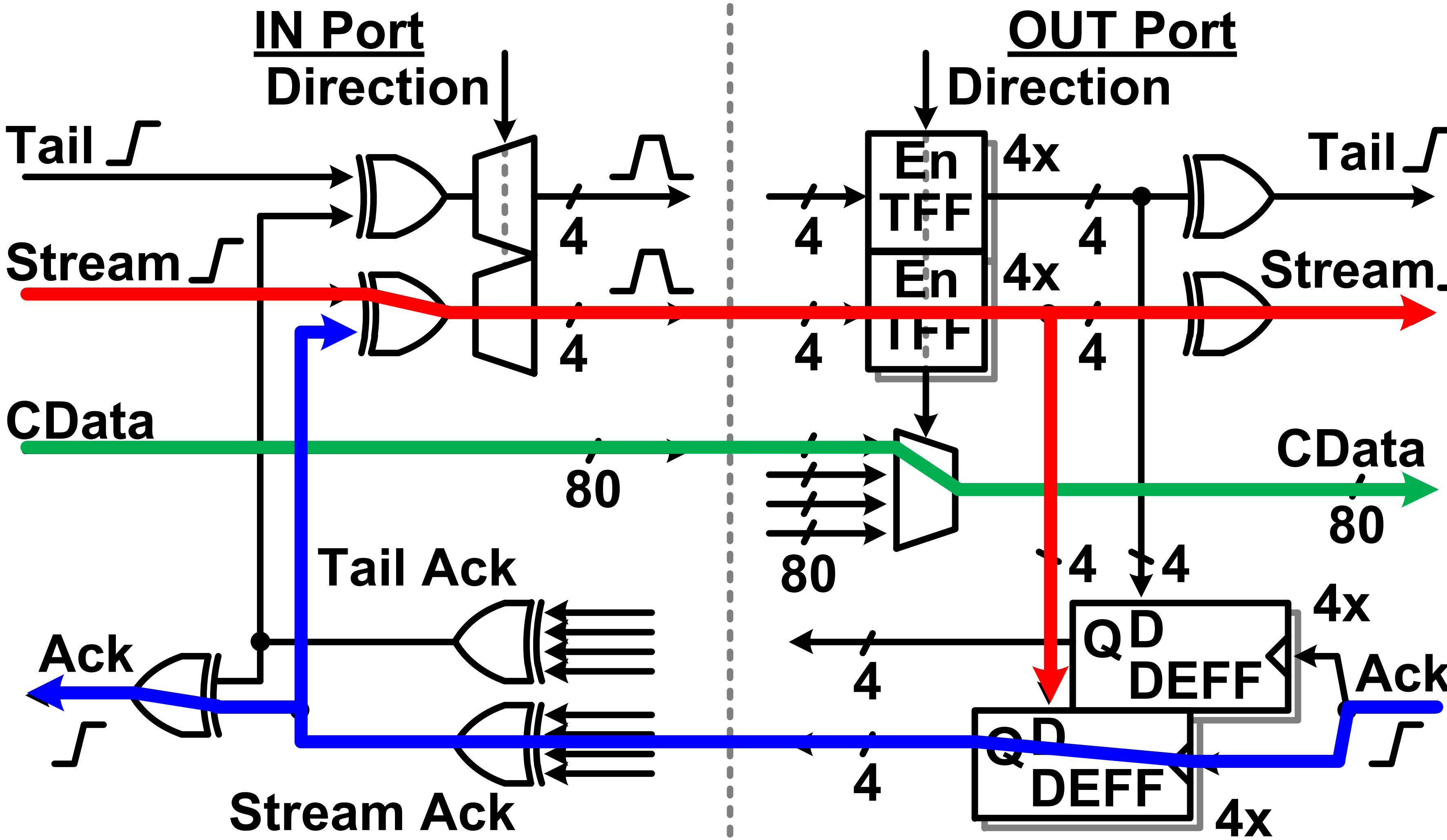
- 3b Gray-counter pointers prevent glitching
- Handles unpredictable signal arrival times
- 4 FIFO entries improve throughput by 75%

Circuit Transfer and Ack Circuits



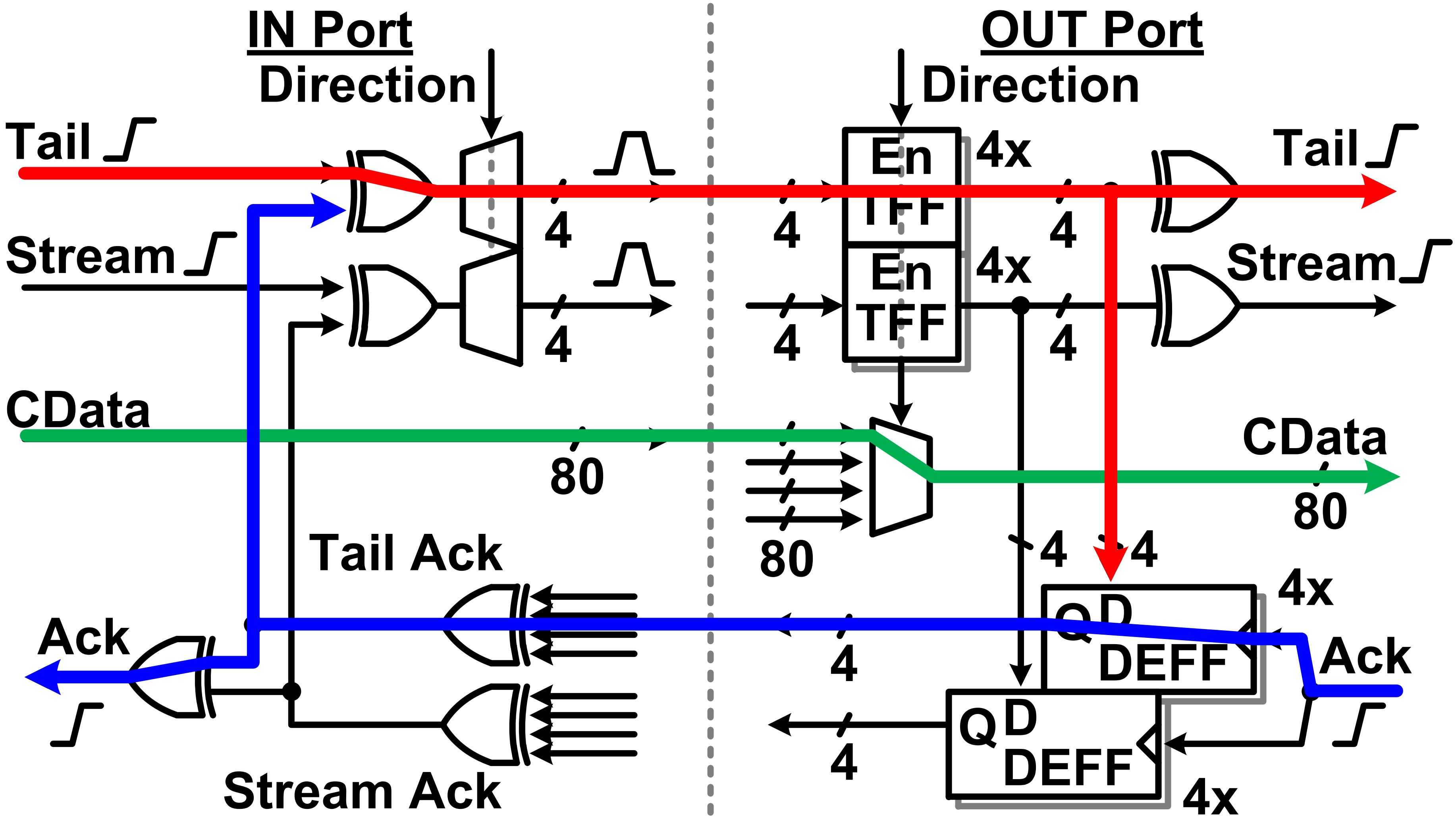
- Direction from FIFO configures channel multiplexers
- Path-specific delay for 93% latency reduction

Circuit Transfer and Ack Circuits



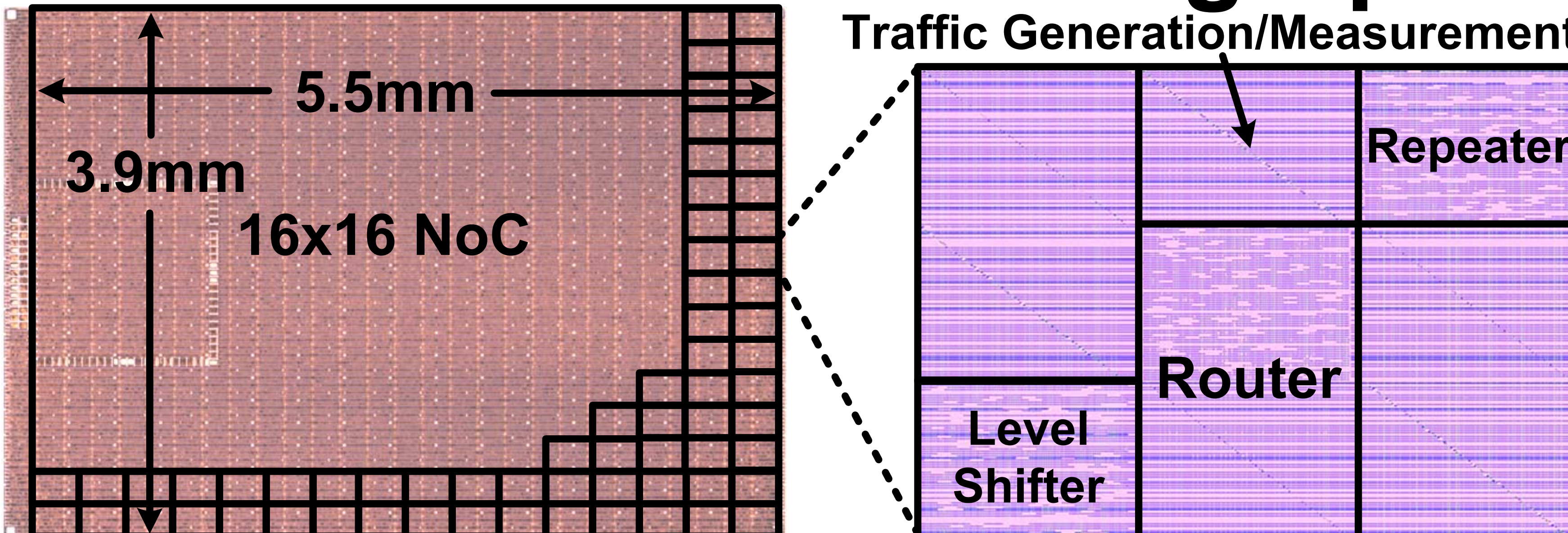
- Direction from FIFO configures channel multiplexers
- Path-specific delay for 93% latency reduction

Circuit Transfer and Ack Circuits



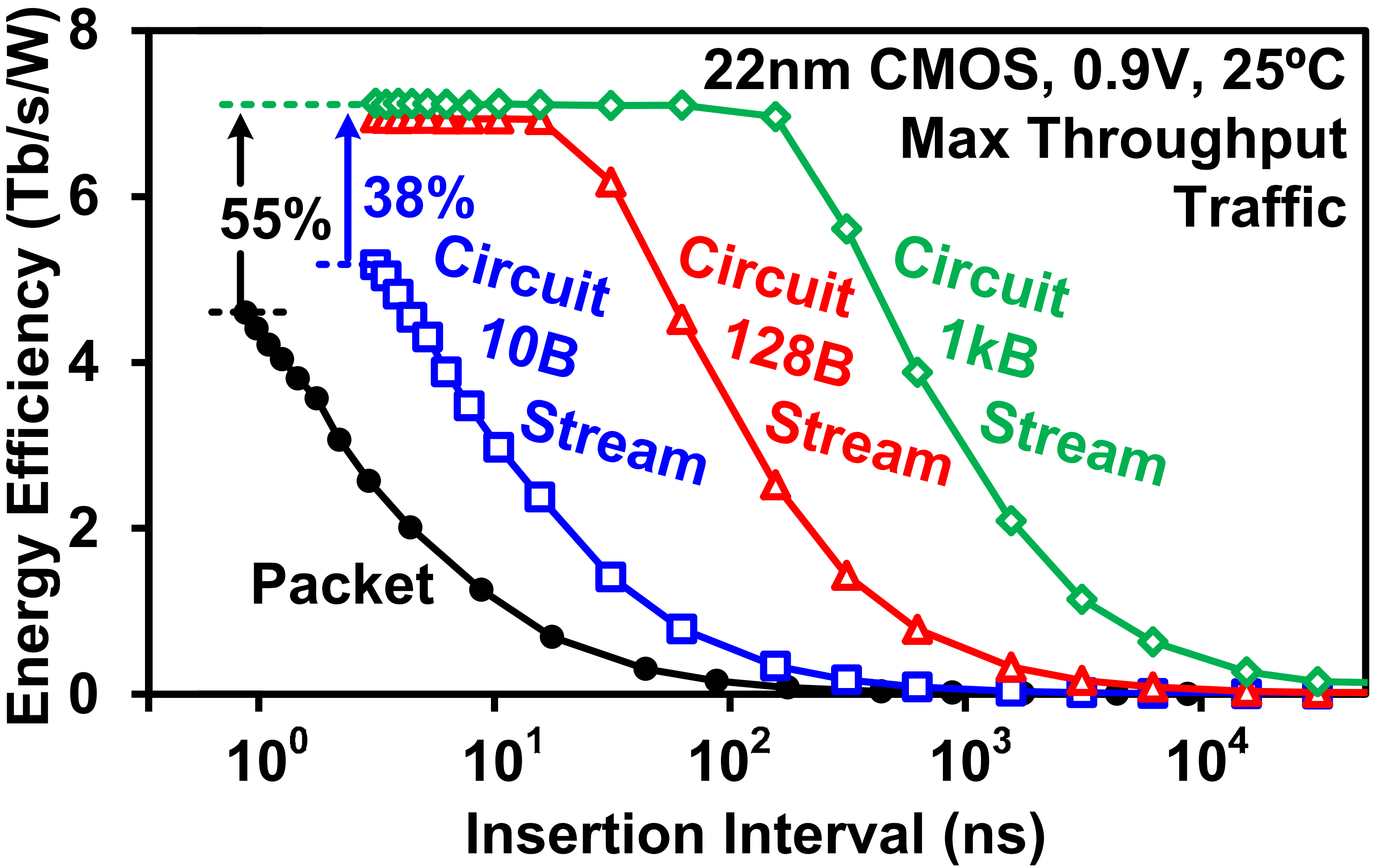
- Direction from FIFO configures channel multiplexers
- Path-specific delay for 93% latency reduction

16x16 NoC Die Micrograph



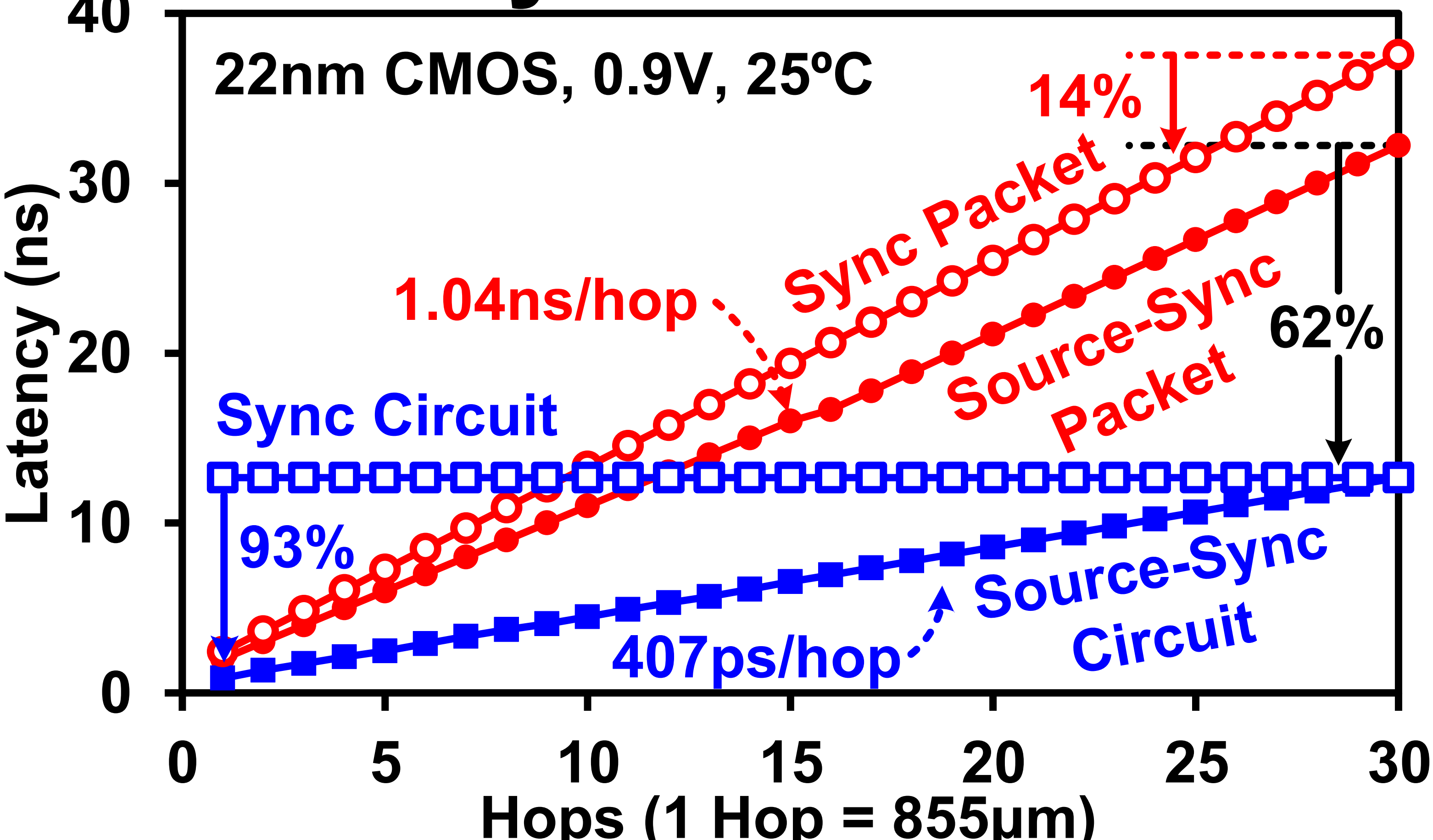
Process	22nm Tri-gate CMOS
Nominal Supply	0.9V
Number of Transistors	150M
Testchip/Equivalent NoC Area	21.5mm^2 / 167mm^2
Router Area	138µm x 109µm
Data Bus Width	112b (80b Circuit/32b Packet)
Interconnect Length	855µm

Insertion Interval Measurements



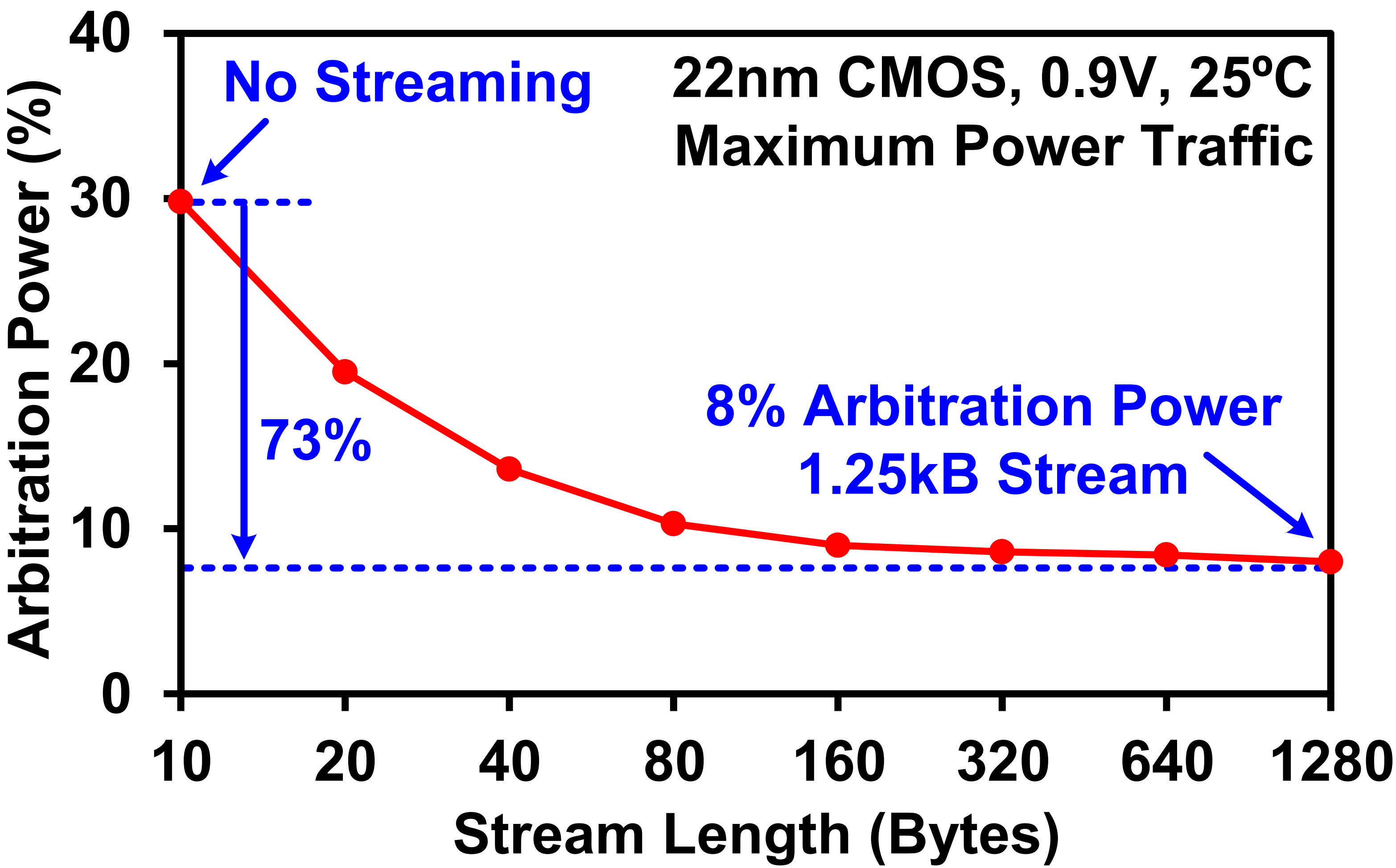
- 32b packet-switched energy efficiency 4.48Tb/s/W
- Circuit switching improves energy efficiency by 55%

Latency Measurements



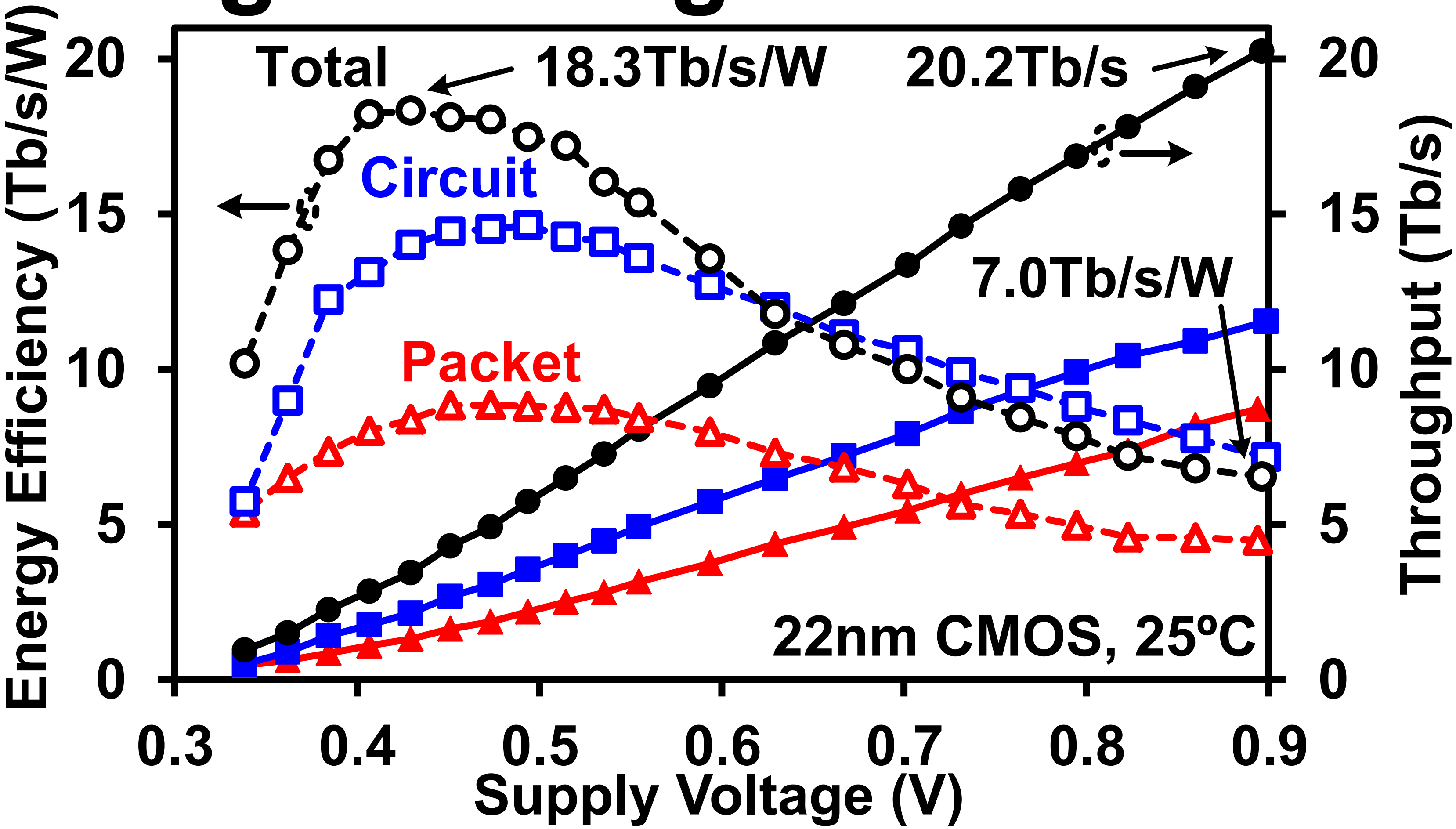
- Delay averaging for 14% packet latency reduction
- Proximity-based delay for 93% lower circuit delay
- 62% faster circuit transfer vs. packet transfer

Streaming Measurements



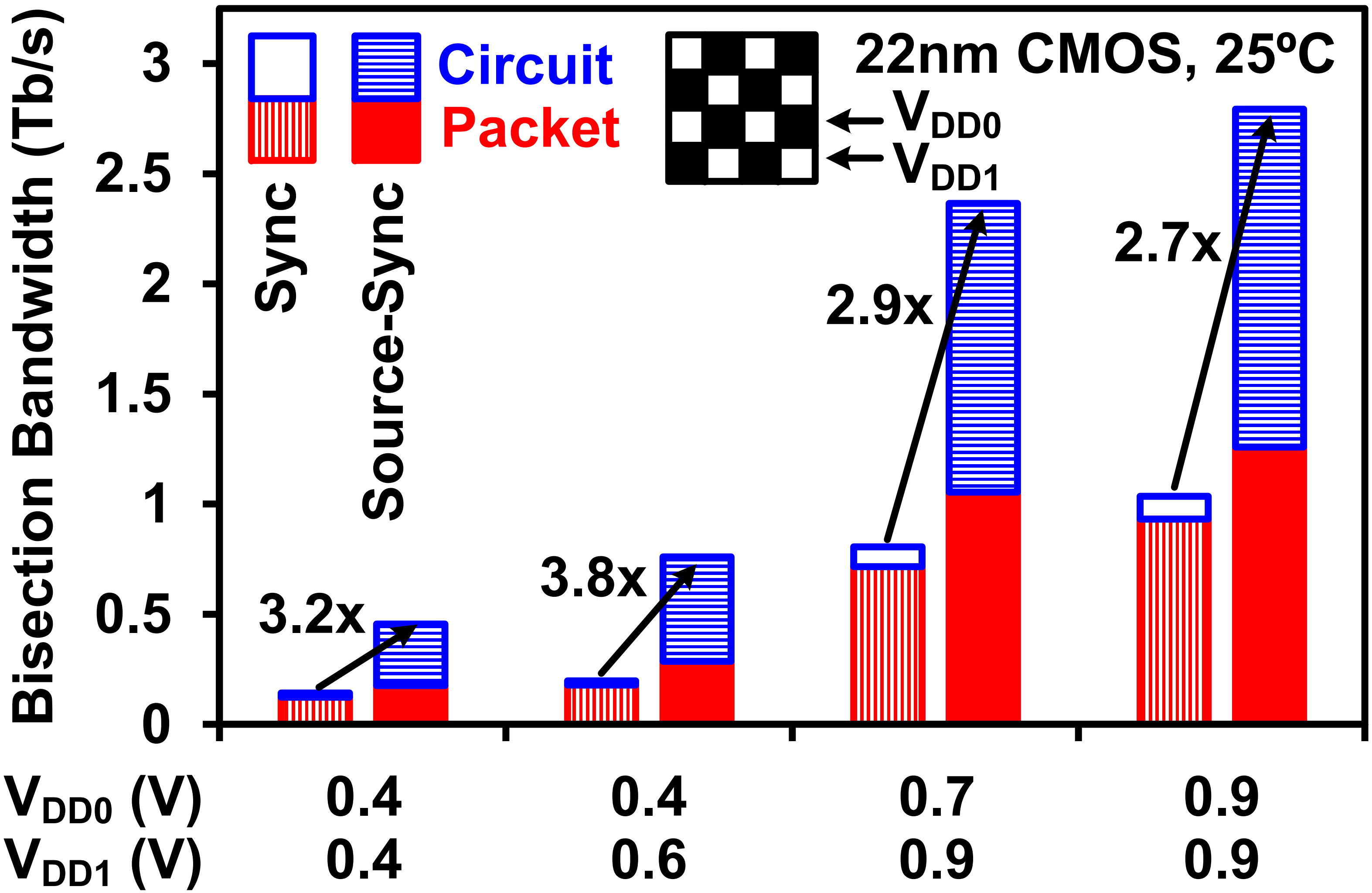
- Amortize setup power and latency over data stream
- 1.25kB transfer lowers arbitration overhead to 8%

Voltage Scaling Measurements



- Performance scales to 20.2Tb/s at 0.9V
- Peak energy efficiency 18.3Tb/s/W at 430mV
- Router power 363μW at 340mV

Multiple Supply Measurements



- 2.7x increase in bisection bandwidth to 2.8Tb/s
- Up to 3.8x higher with multiple supply voltages

Summary

- 16x16 2D-mesh NoC in 22nm tri-gate CMOS

- Source-synchronous for variation tolerance
  - 20.2Tb/s total throughput
  - 2.7x increase in bisection bandwidth to 2.8Tb/s

- Hybrid packet/circuit-switching lowers energy
  - 55% increase in energy efficiency to 7.0Tb/s/W

- Wide supply voltage range 340mV-0.9V
  - Peak energy efficiency 18.3Tb/s/W at 430mV

A 0.19pJ/bit PVT Variation-Tolerant Hybrid Physically Unclonable Function Circuit for 100% Stable Secure Key Generation in 22nm CMOS

Sanu K. Mathew, Sudhir K. Satpathy, Mark A. Anders, Himanshu Kaul, Amit Agarwal, Steven K. Hsu, Gregory K. Chen, Rachael J. Parker, Ram K. Krishnamurthy, Vivek De

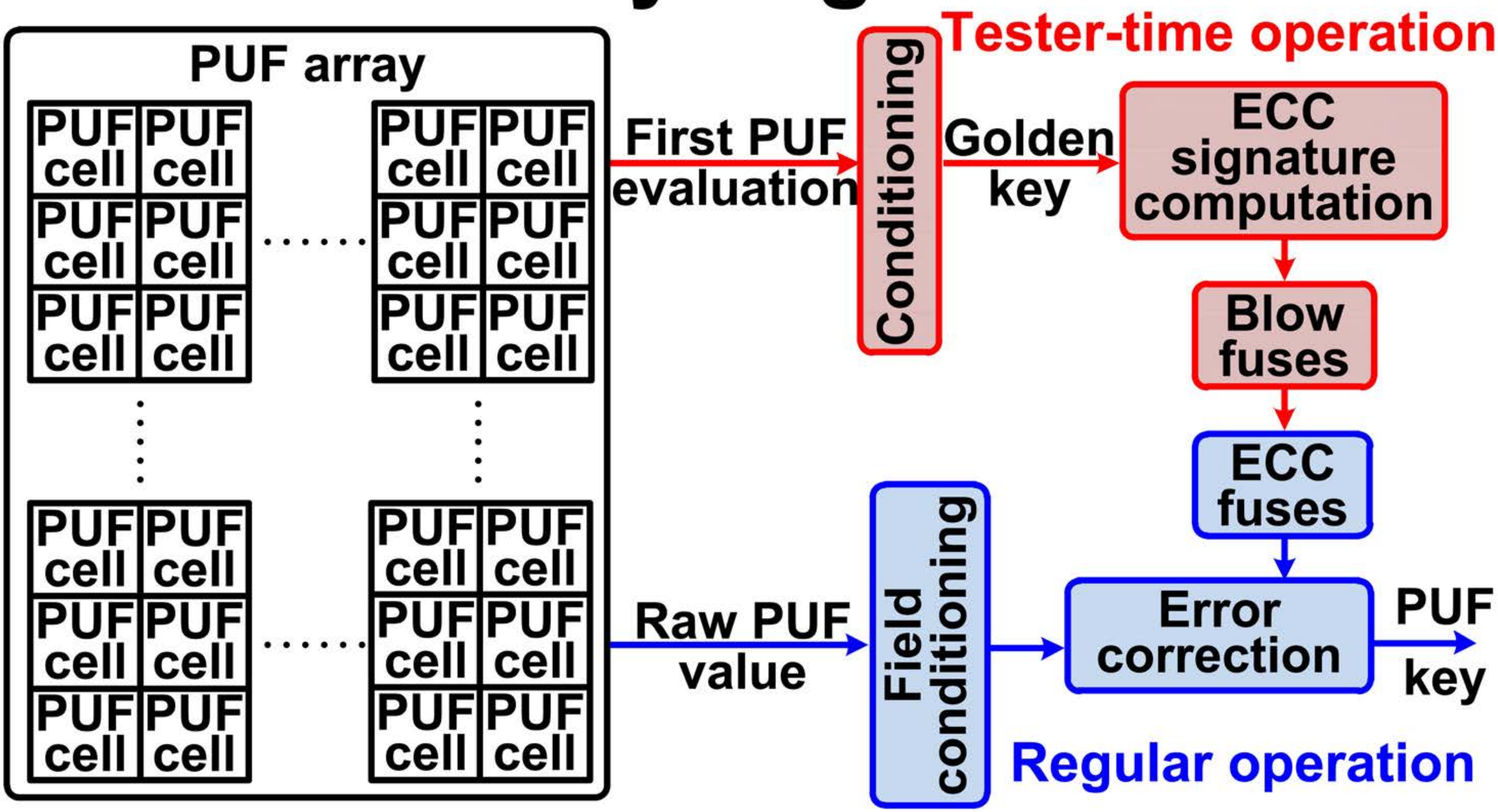
Circuit Research Lab, Intel Corporation

Hillsboro, OR, U.S.A.

Outline

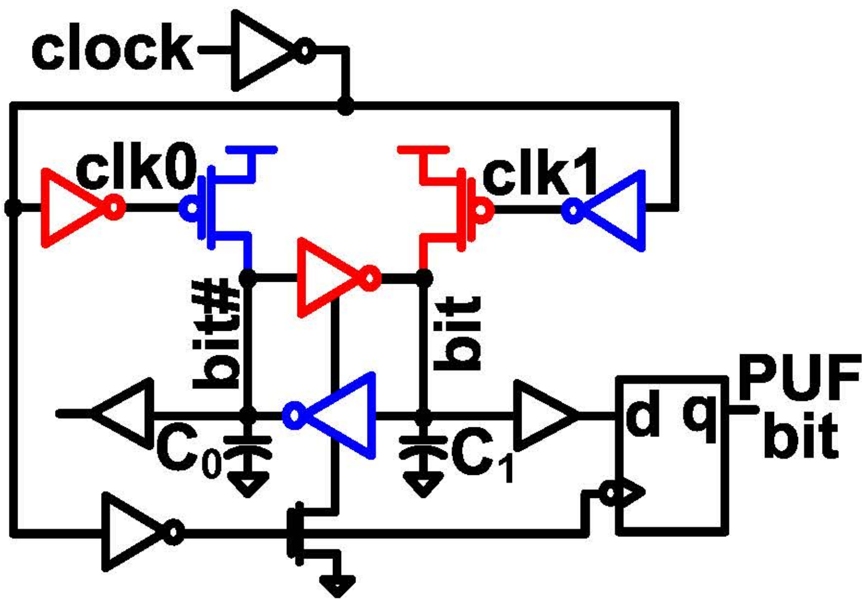
- Physically Unclonable Function (PUF) array organization
- Hybrid PUF circuit
- TMV, burn-in hardening and soft dark bits
- PUF measurements in 22nm CMOS
- PUF variation tolerance measurements
- Summary

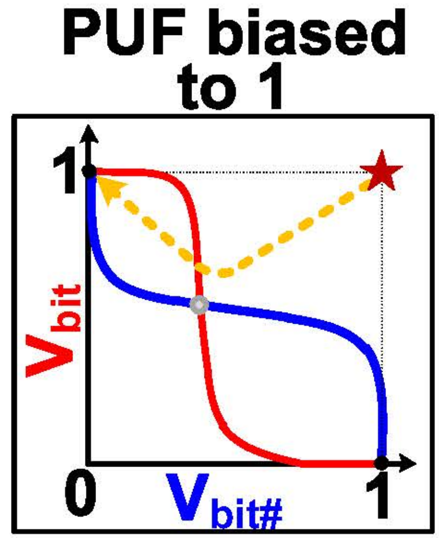
PUF Array Organization

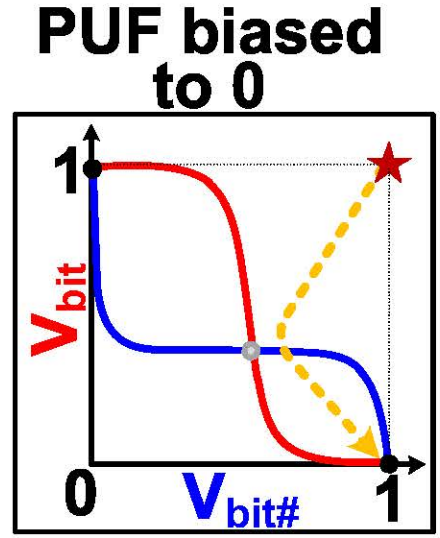


- Goal: stable and repeatable device-specific secure key
- ECC of golden key computed and burned into fuses
- Raw PUF + on-die correction ⇒ 100% stable PUF key

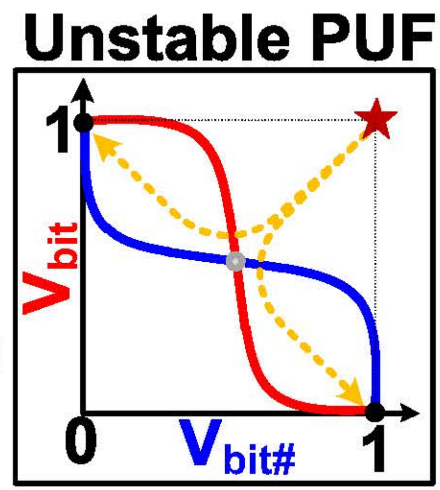
Hybrid PUF Circuit



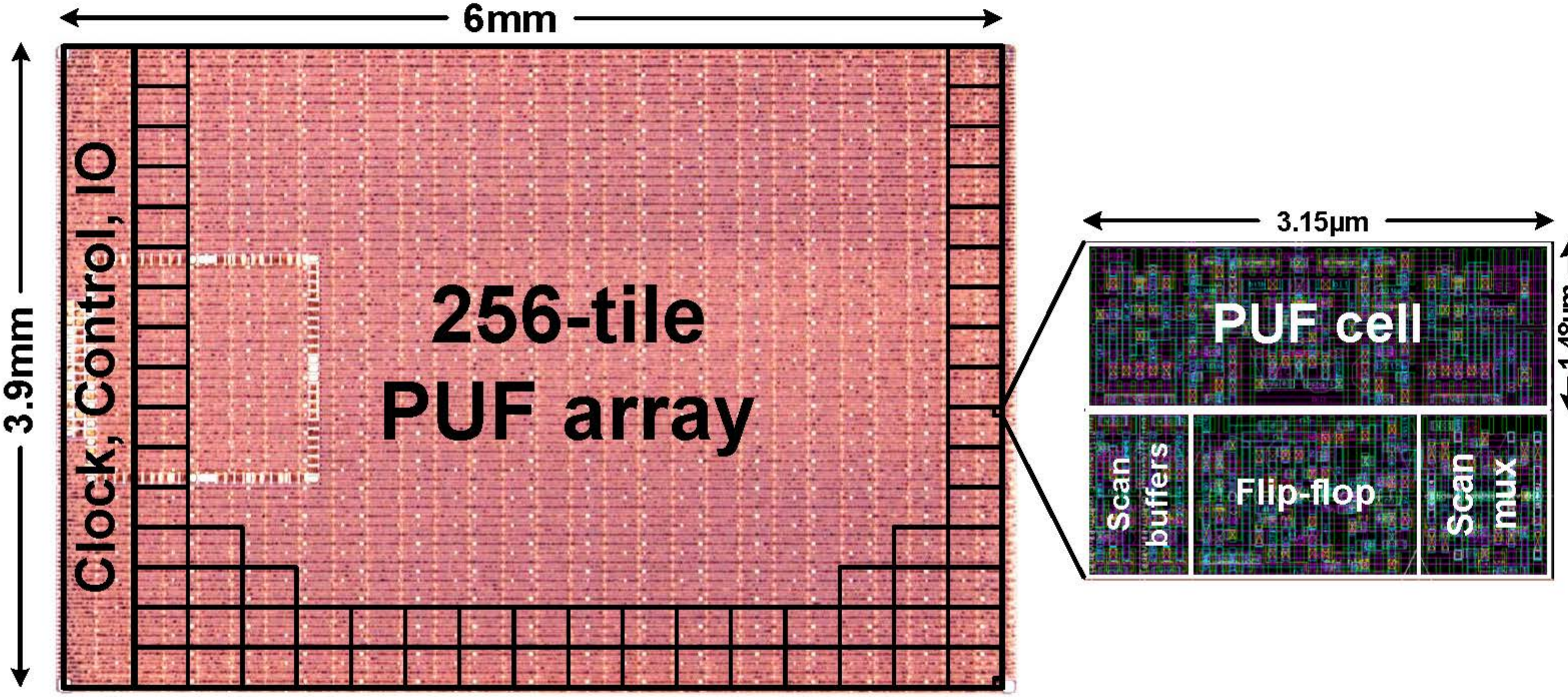




- PUF resolves from unstable state due to:
  - Random variation in inverter devices
  - Clock rise delay/arrival time mismatch
- 10 minimum-sized devices determine resolution dynamics

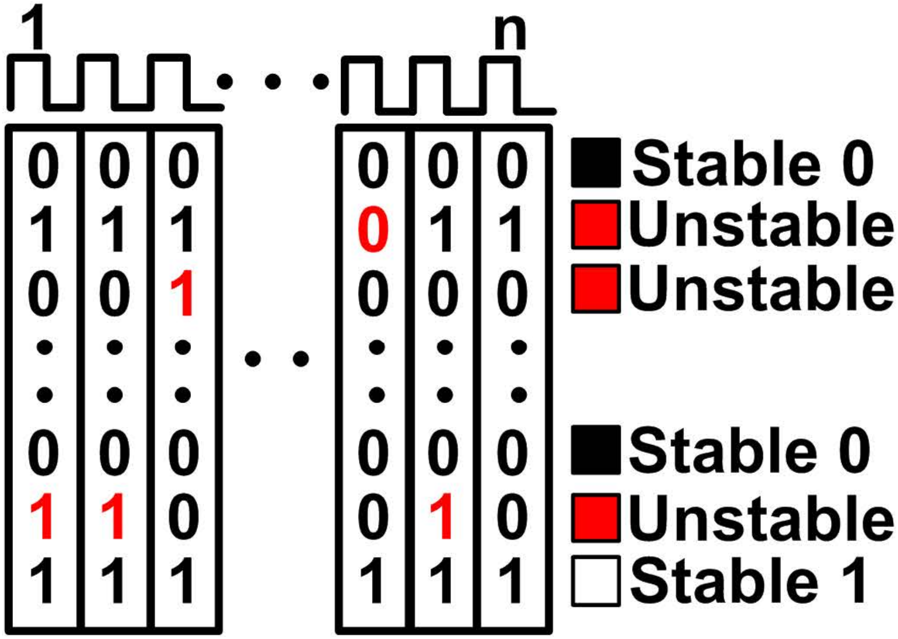


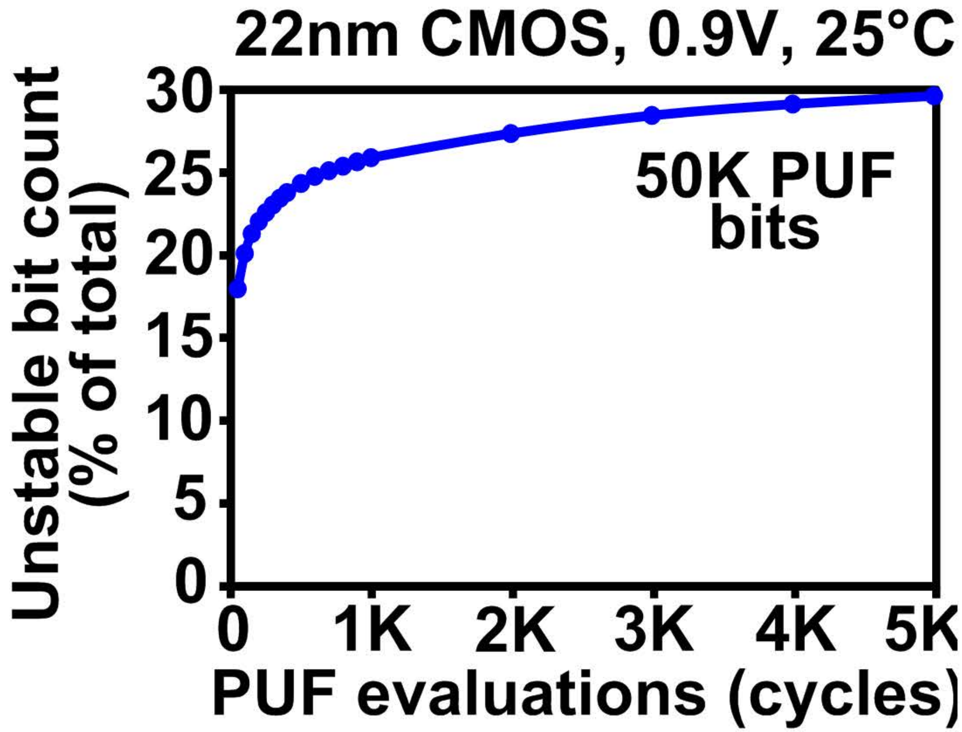
Die Micrograph & 22nm Layout



Process	22nm tri-gate high-K metal gate CMOS
Die area	$24mm^2$
Bitcell area	$4.66\mu m^2$
Array organization	256x196

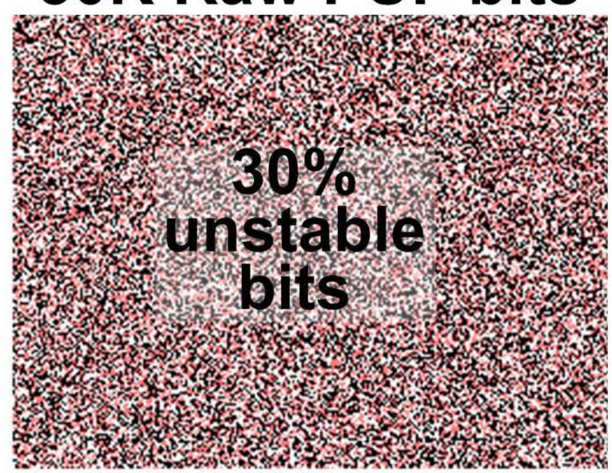
Raw PUF Stability Measurements



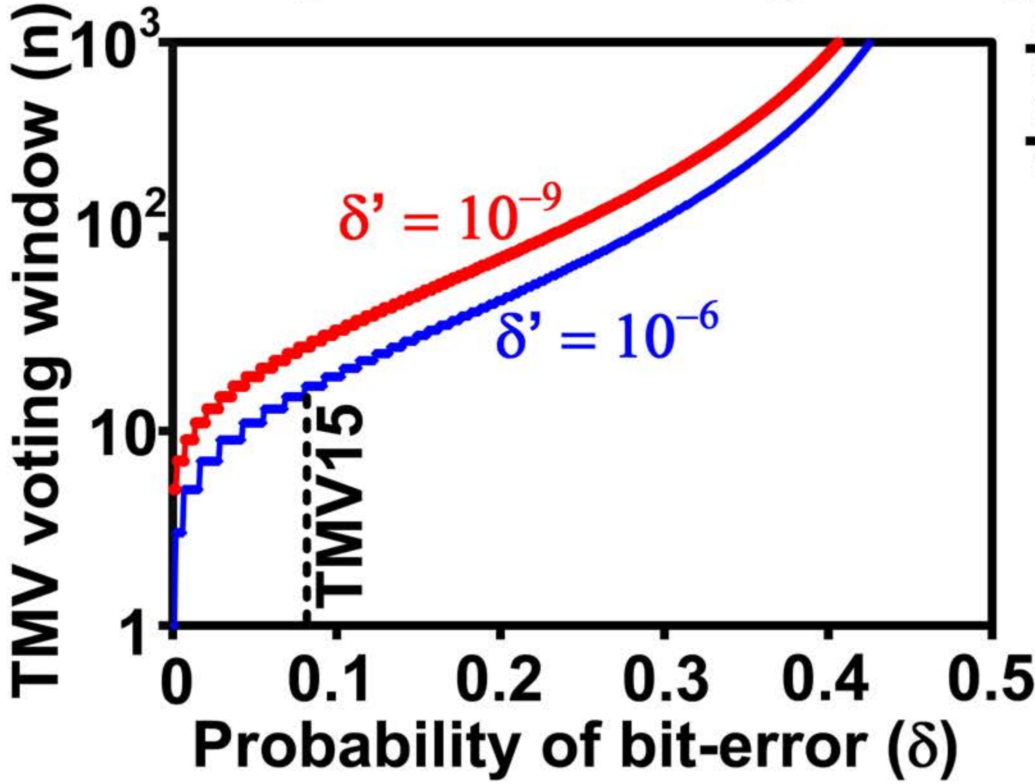


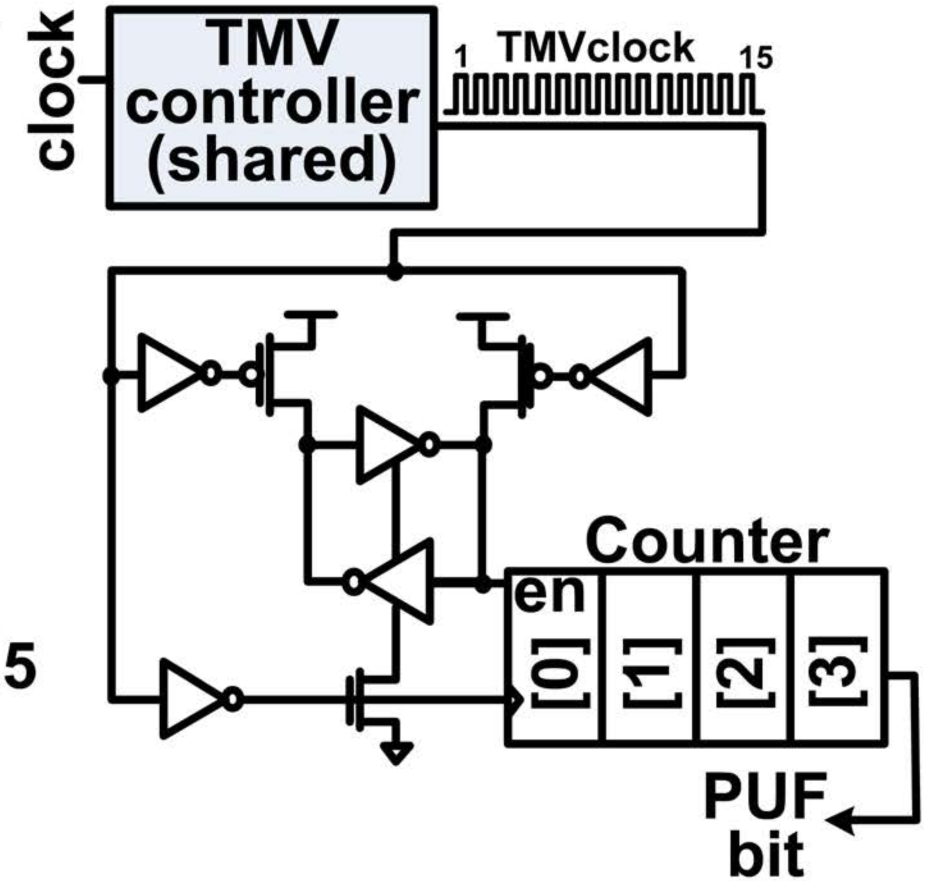
- Evaluate PUF over multiple cycles
- Count=0 or n ⇒ Stable bit
- 0<Count<n ⇒ Unstable bit
- 30% of PUF bits are unstable after 5000 cycles

50K Raw PUF bits



Temporal Majority Voting Circuit

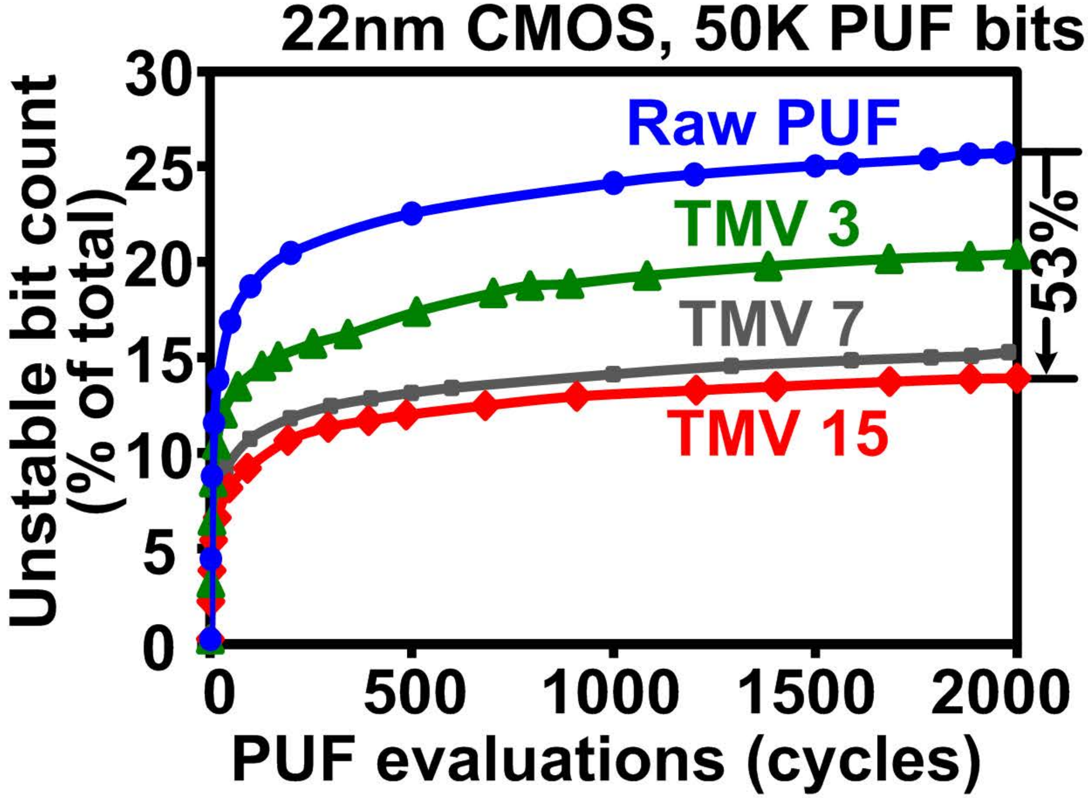




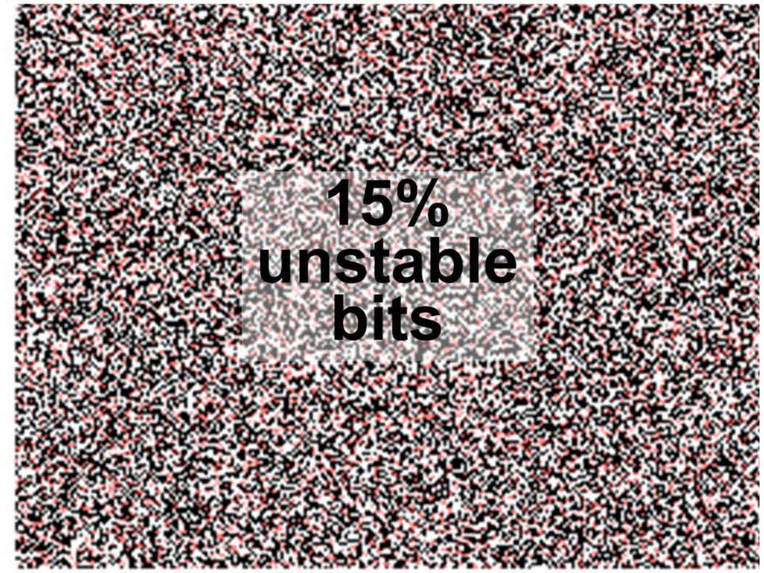
$$\delta' = 1 - \sum_{i=1}^{(n-1)/2} \delta^i.(1-\delta)^{n-i}.{}^nC_i$$

- Computes quantized mean of PUF response in voting window (width=3, 7, 15)
- TMV15 fixes mildly unstable bits (δ<0.08)

TMV Measurements

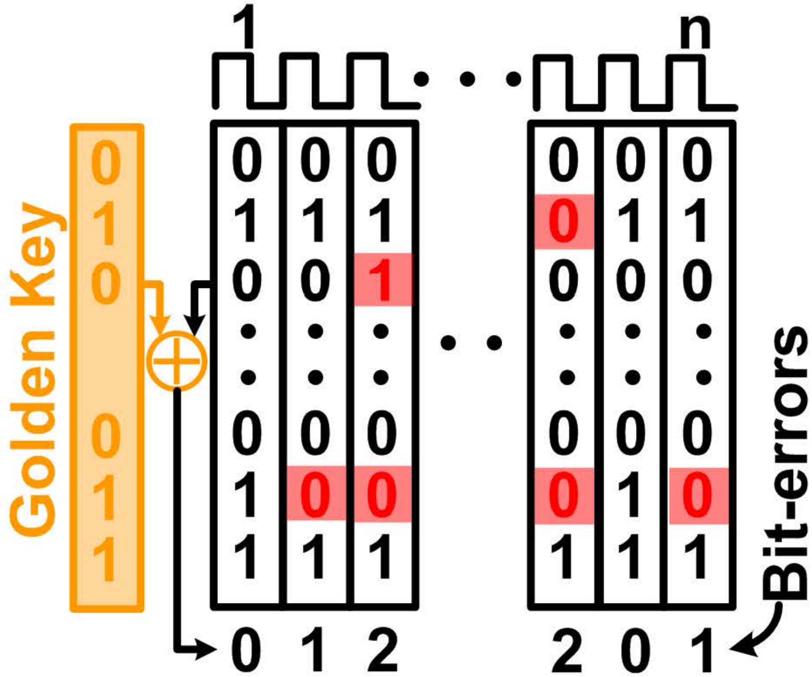


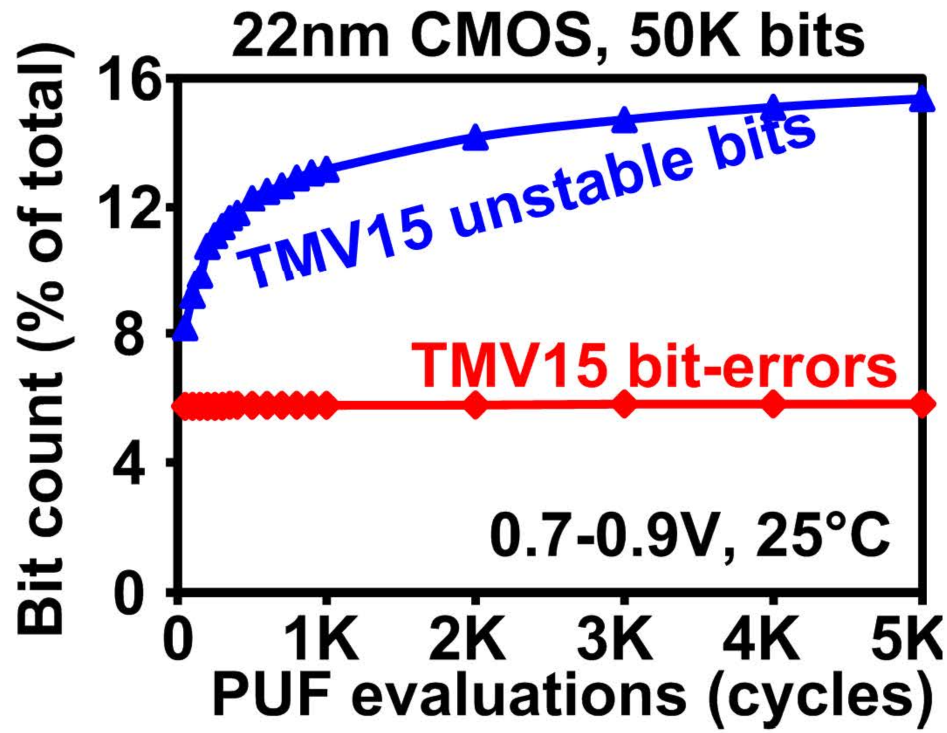
Unstable bits with TMV15



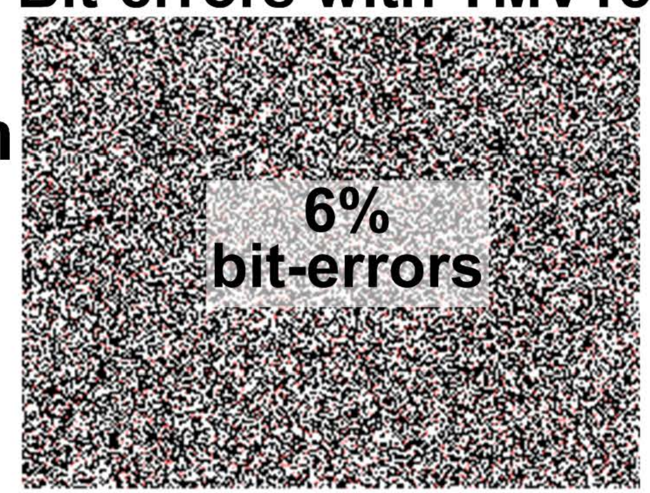
- 53% reduction in unstable bit count
- TMV effectiveness decreases at wider voting windows
- TMV15 reduces unstable bit count to 15%

PUF Bit-error Measurements



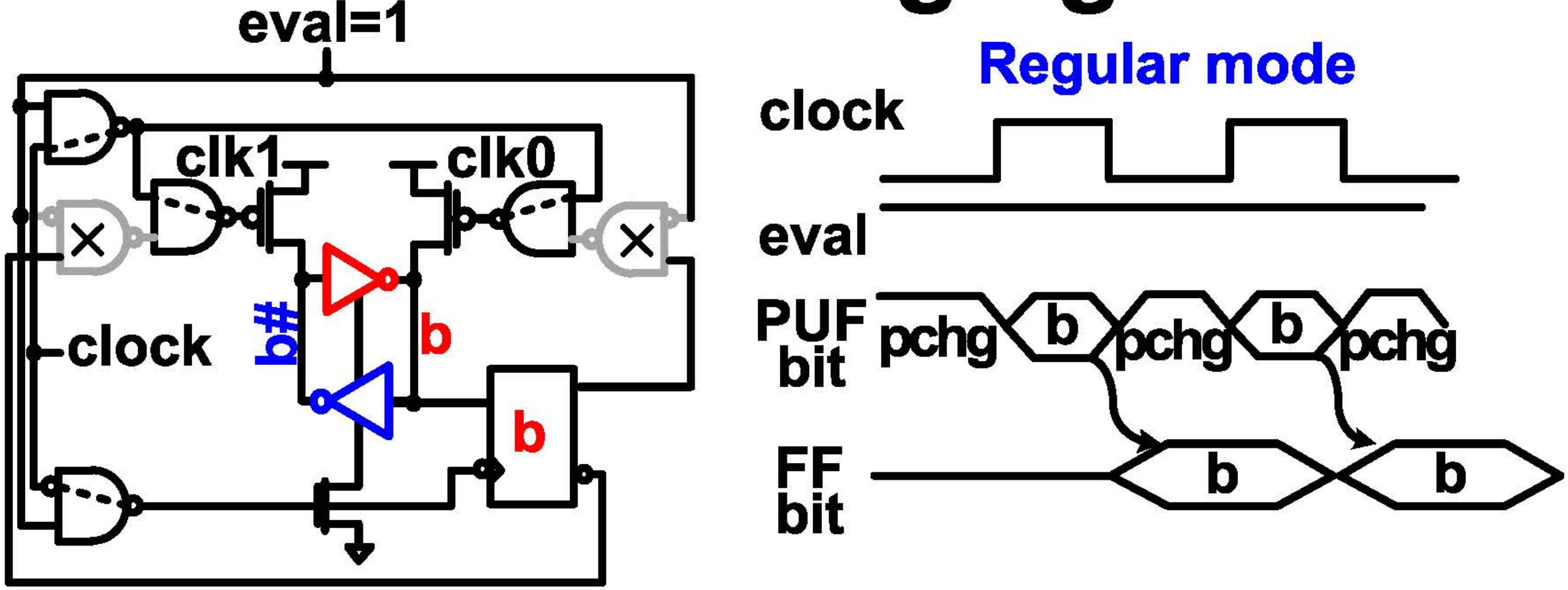


Bit-errors with TMV15



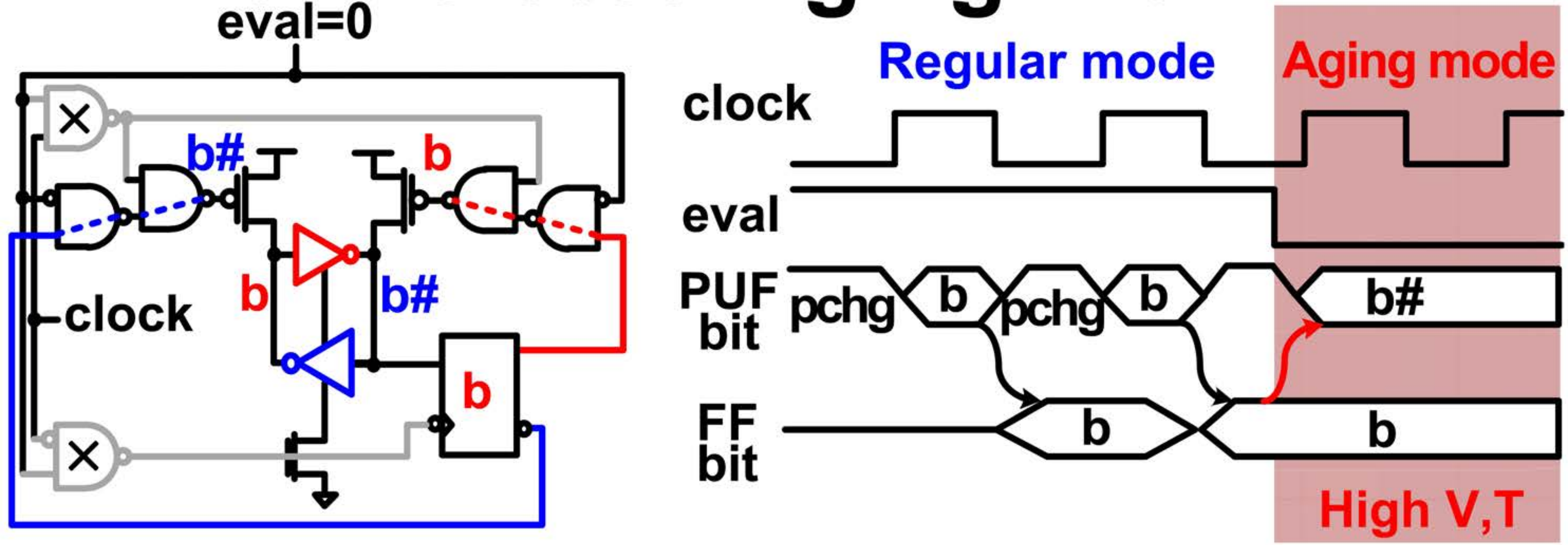
- Golden key created at first evaluation
- 43% unstable bits do not match golden key ⇒ bit-errors
- ECC is used to correct bit-errors

Accelerated Aging: Burn-in



- Improves stability by reinforcing existing cell bias
- Clock inverters replaced by NAND gates
- eval=1 $\Rightarrow$ regular mode of operation
- PUF bit written into flip-flop

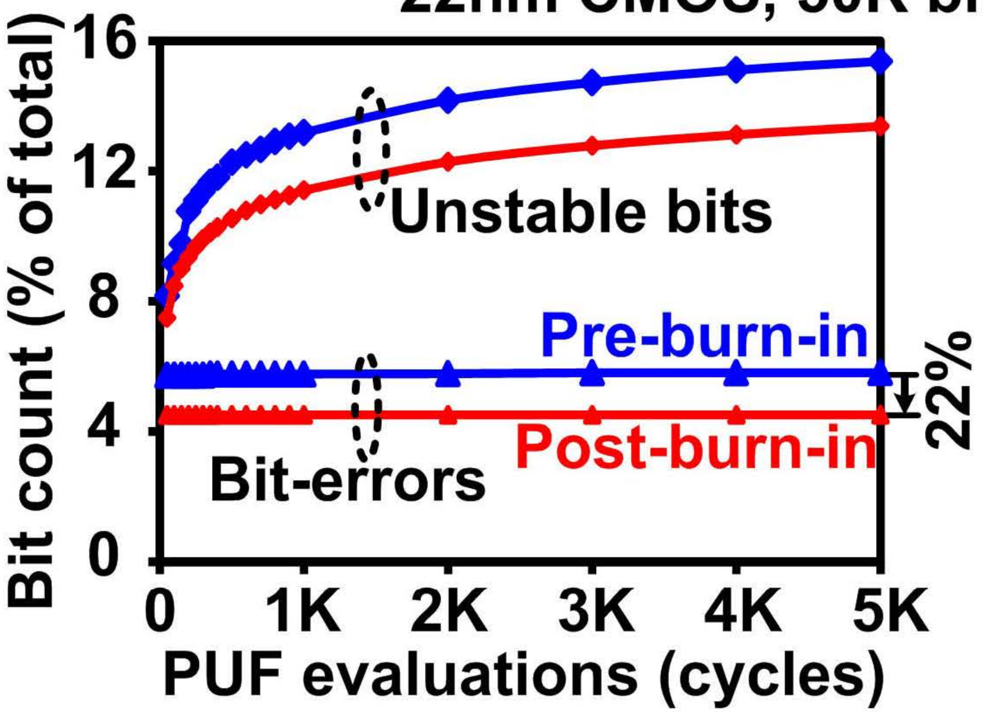
Accelerated Aging: Burn-in



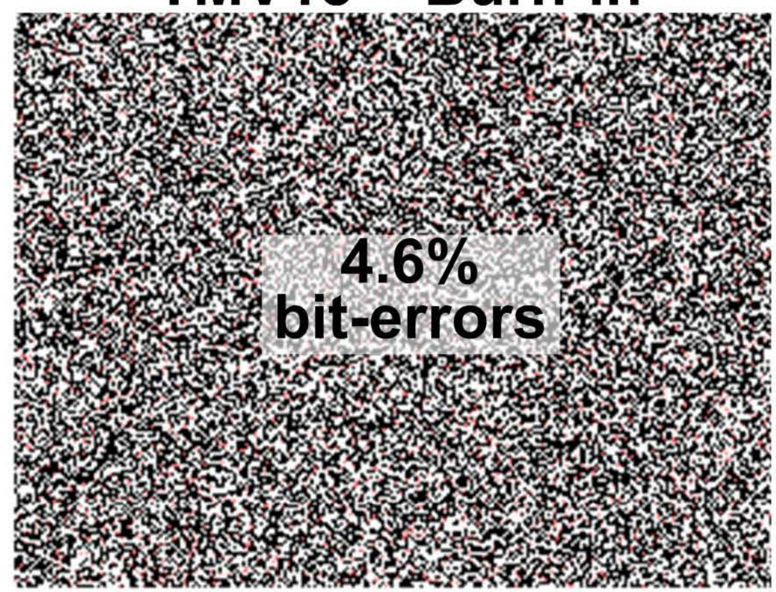
- eval=0 ⇒ aging mode, die subjected to burn-in
- Clock is gated, feedback NAND gates are transparent
- Complementary PUF value written back into PUF cell
- Inverter and clock devices biased to age in the direction favoring stability

PUF Post-Burn-in Measurements

22nm CMOS, 50K bits, 0.7-0.9V, 25°C

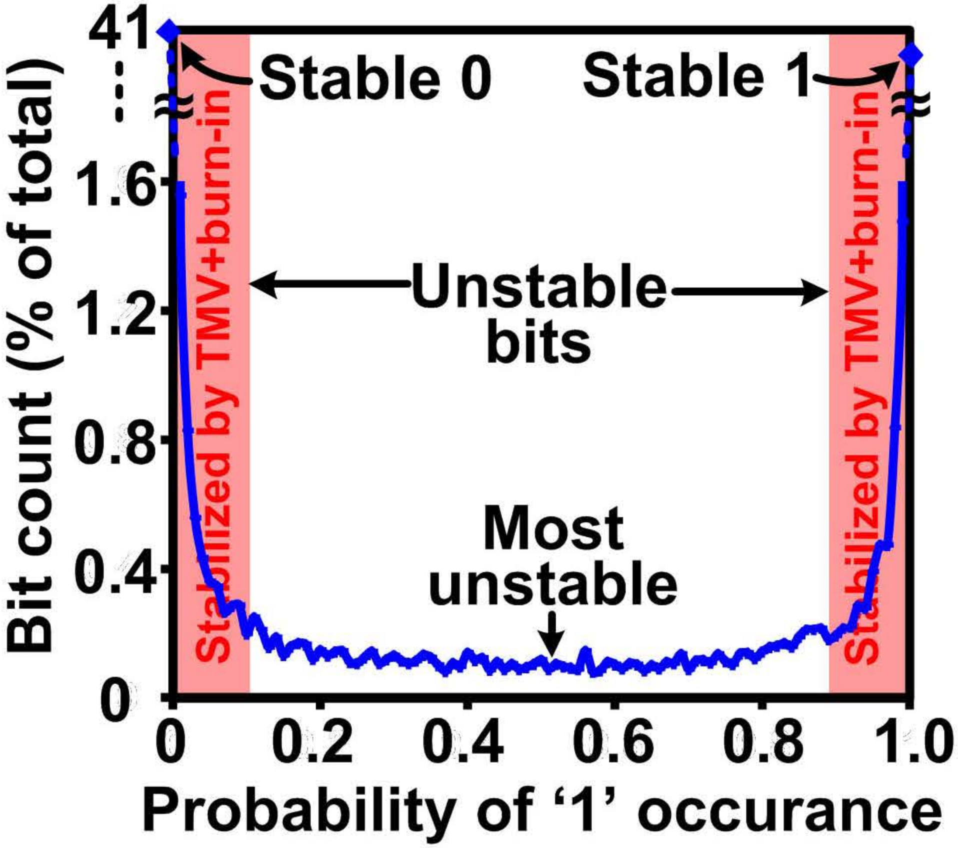


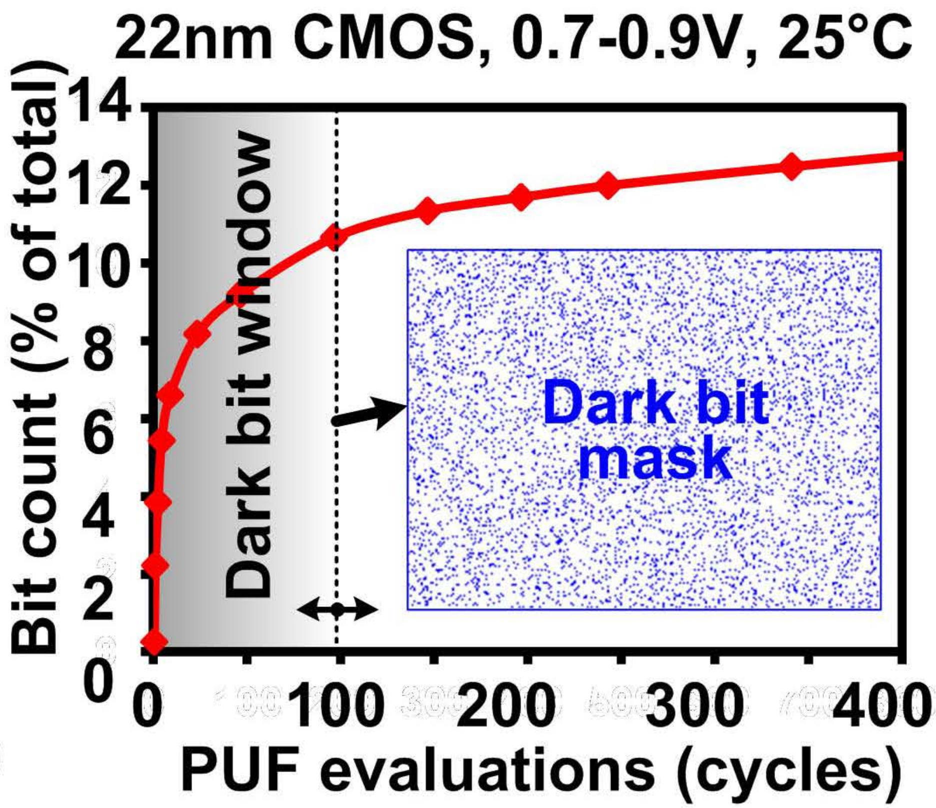
TMV15 + Burn-in



- Burn-in reinforces golden key bias
  - Stabilizes mildly unstable PUF bits
- 22% reduction in bit-errors
- In-situ hardening counters long-term aging

Soft Dark Bits

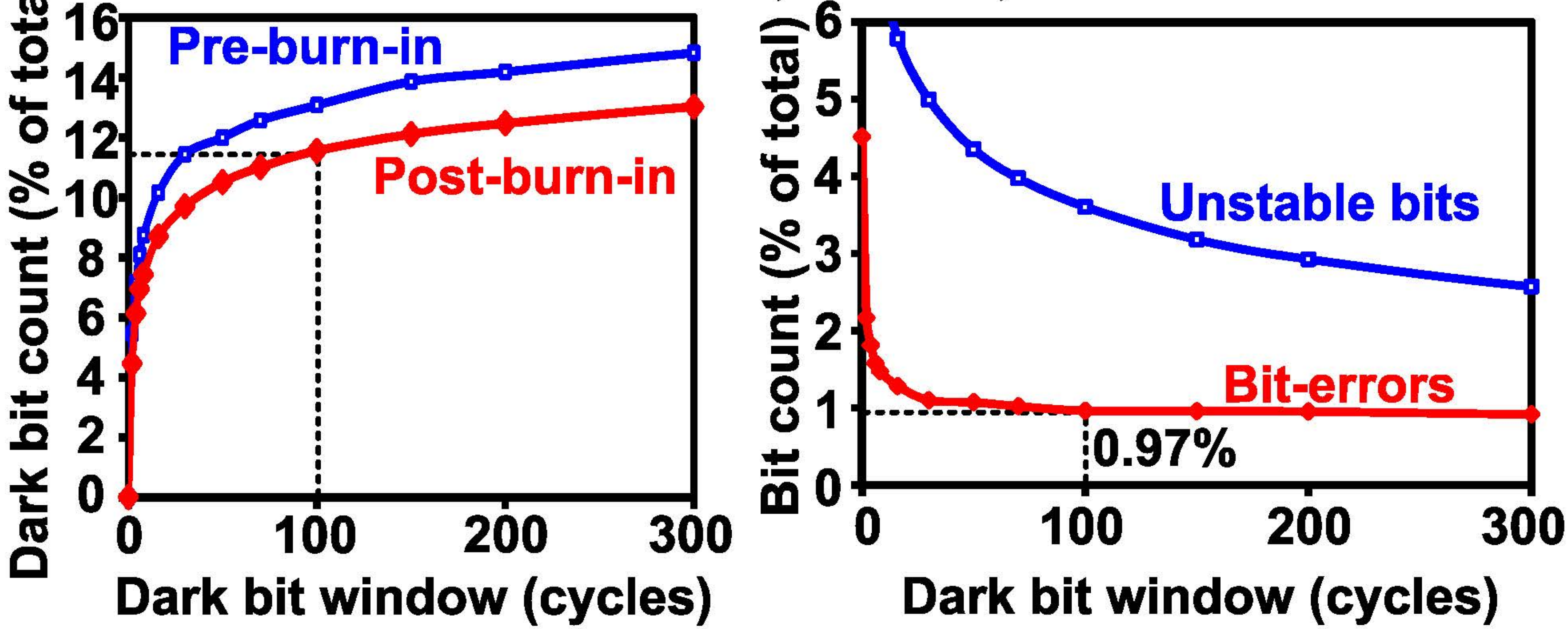




- TMV15+burn-in stabilizes 57% of unstable bits
  - Ineffective on remaining highly unstable bits
- Detect and generate soft mask at each startup
  - Sets all dark bits to '0'

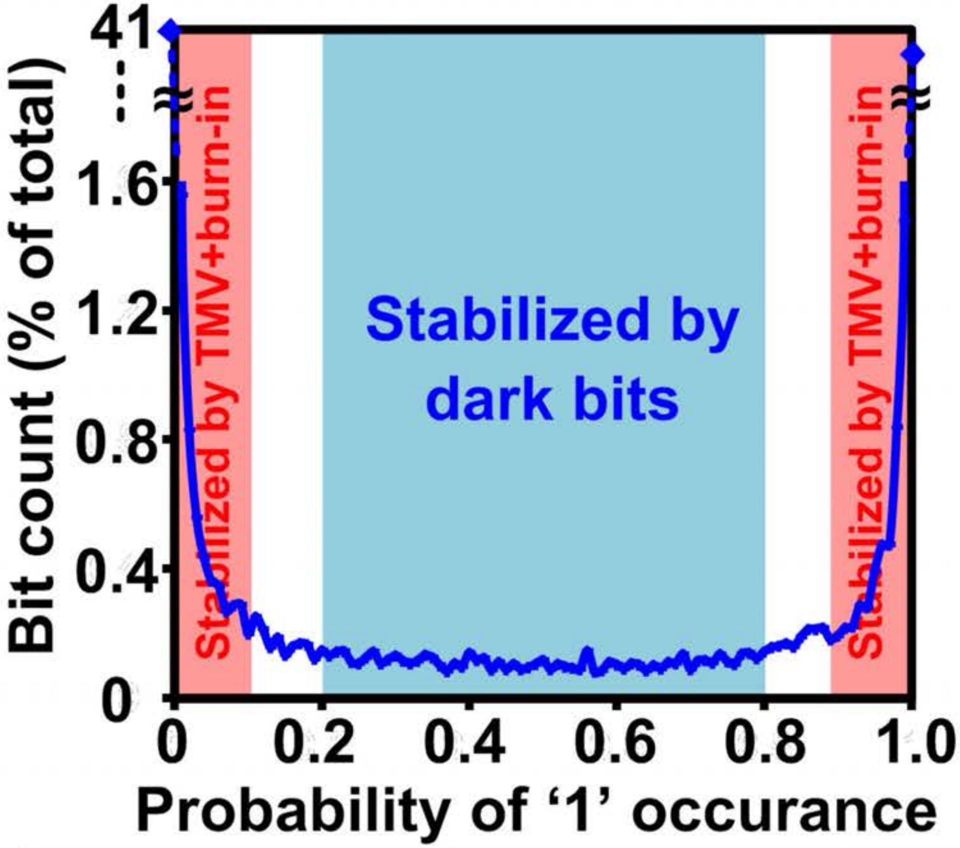
Soft Dark Bit Measurements

22nm CMOS, 0.7-0.9V, 25°C

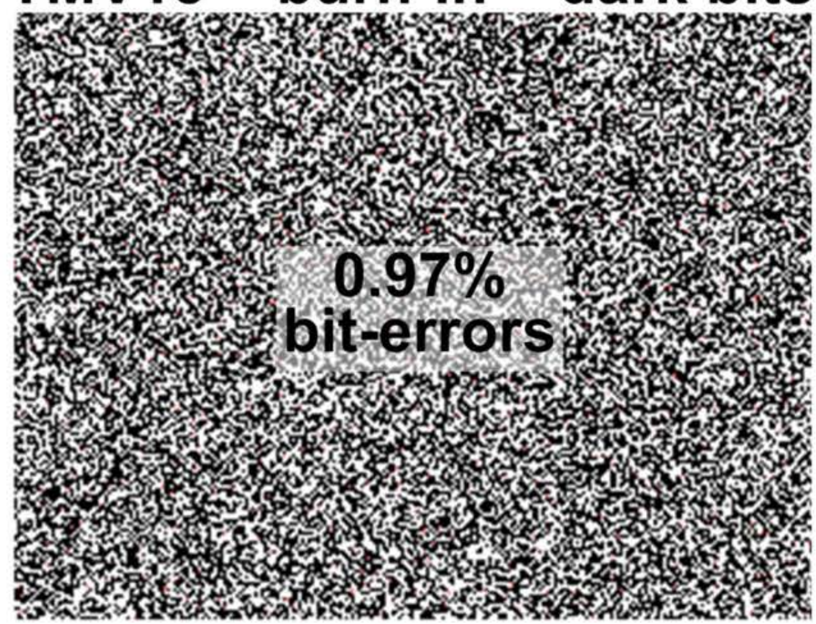


- Optimal dark bit window is ~100 cycles
- 11% of total bits masked to ‘0’
- Bit-errors reduced to 0.97% of total bits

Soft Dark Bit Measurements



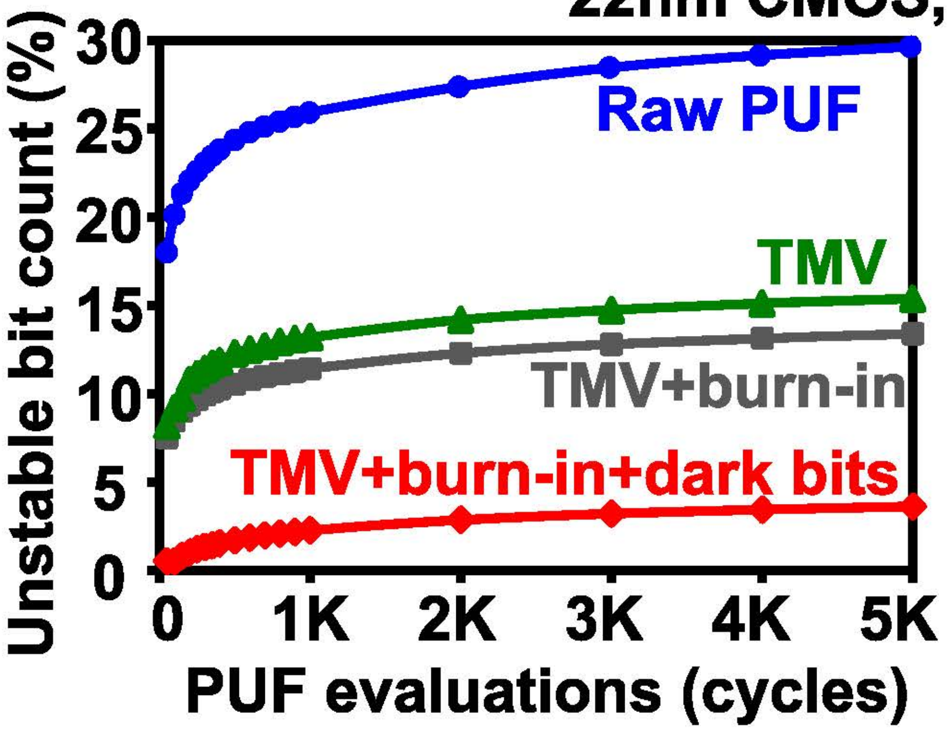
22nm CMOS, 0.7-0.9V, 25°C
TMV15 + burn-in + dark bits

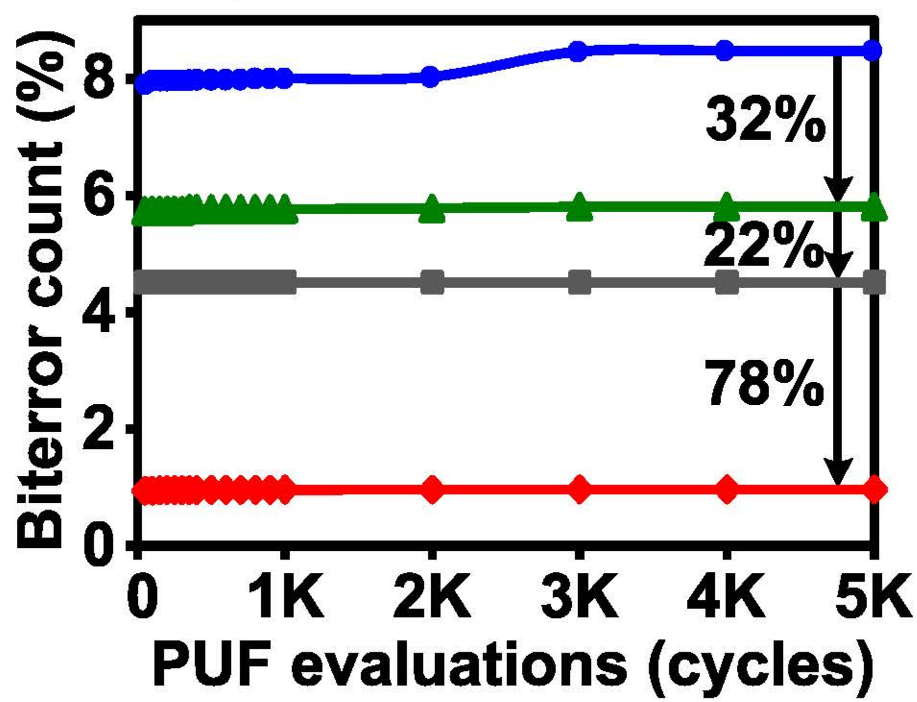


Probability of ‘1’		Error probability	Stabilization
0<P(1)<0.1	0.9<P(1)<1	0<δ<0.1	TMV15 + burn-in
0.2<P(1)<0.8		0.2<δ<0.5	Soft dark bits
0.1<P(1)<0.2	0.8<P(1)<0.9	0.1<δ<0.2	ECC

PUF Stabilization Summary

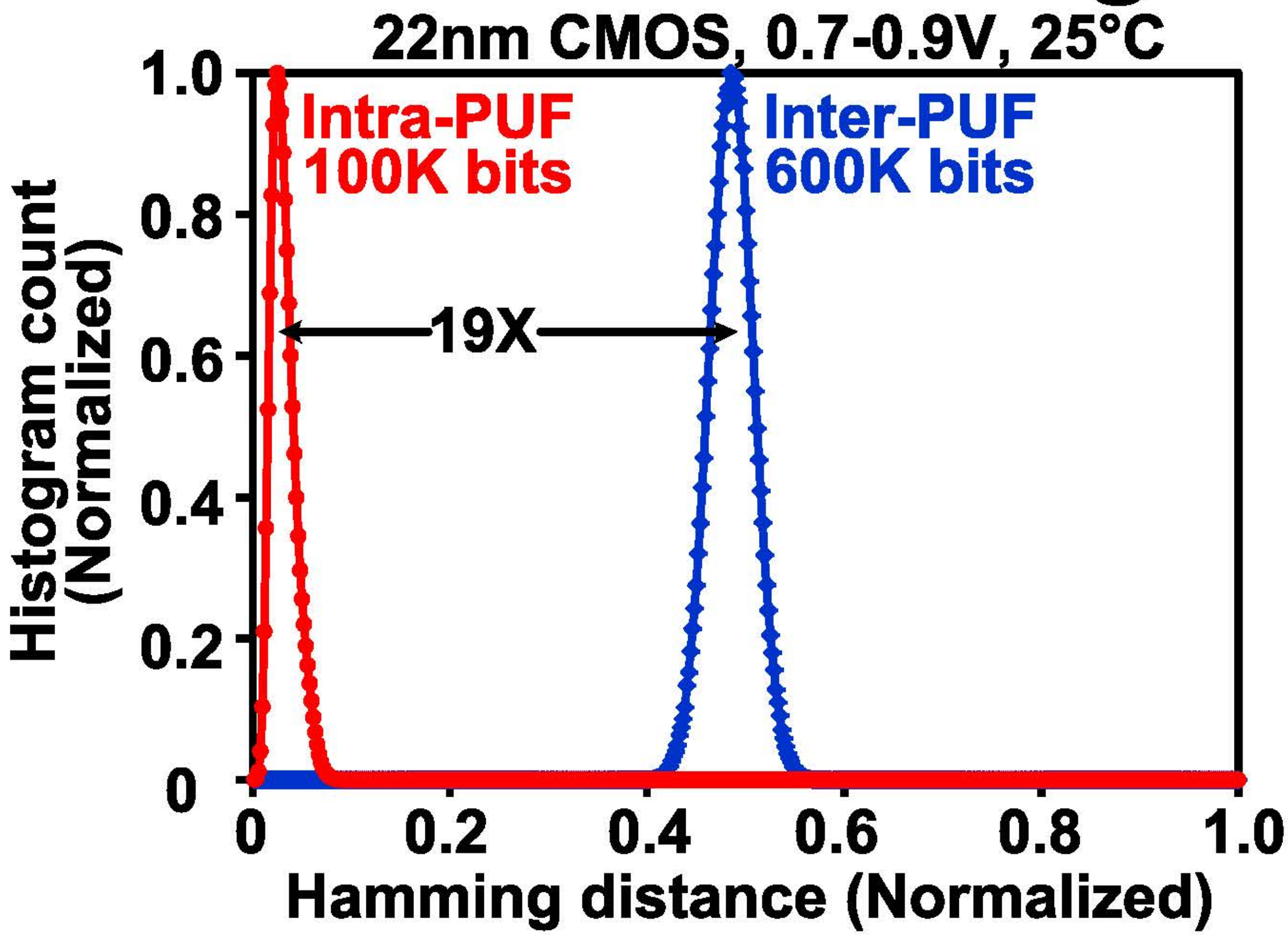
22nm CMOS, 0.7-0.9V, 25°C





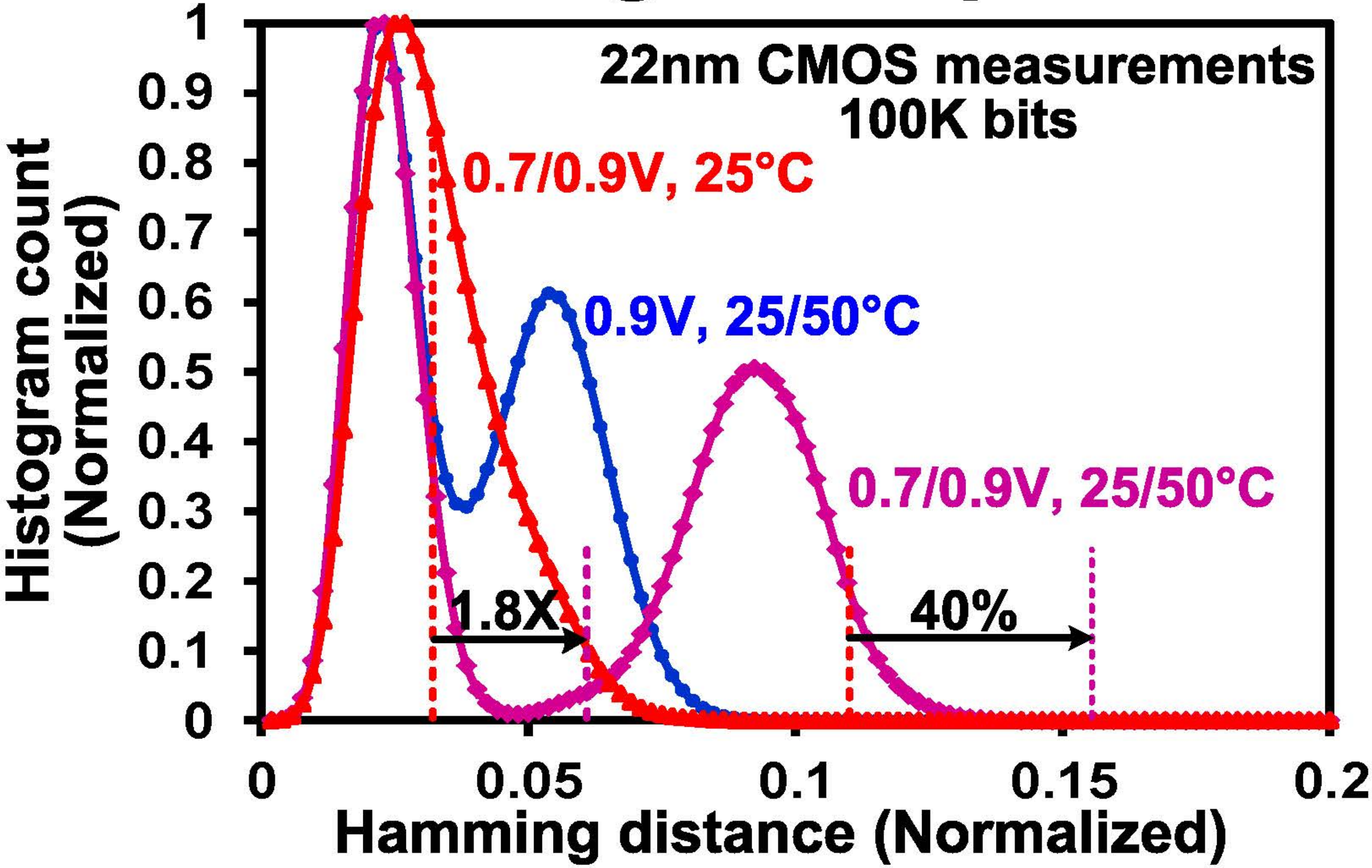
- 3 PUF stabilizations techniques: TMV, burn-in, dark bits
- Overall bit-error rate reduced to 0.97% (8X reduction)

Inter/Intra-PUF Hamming Distance



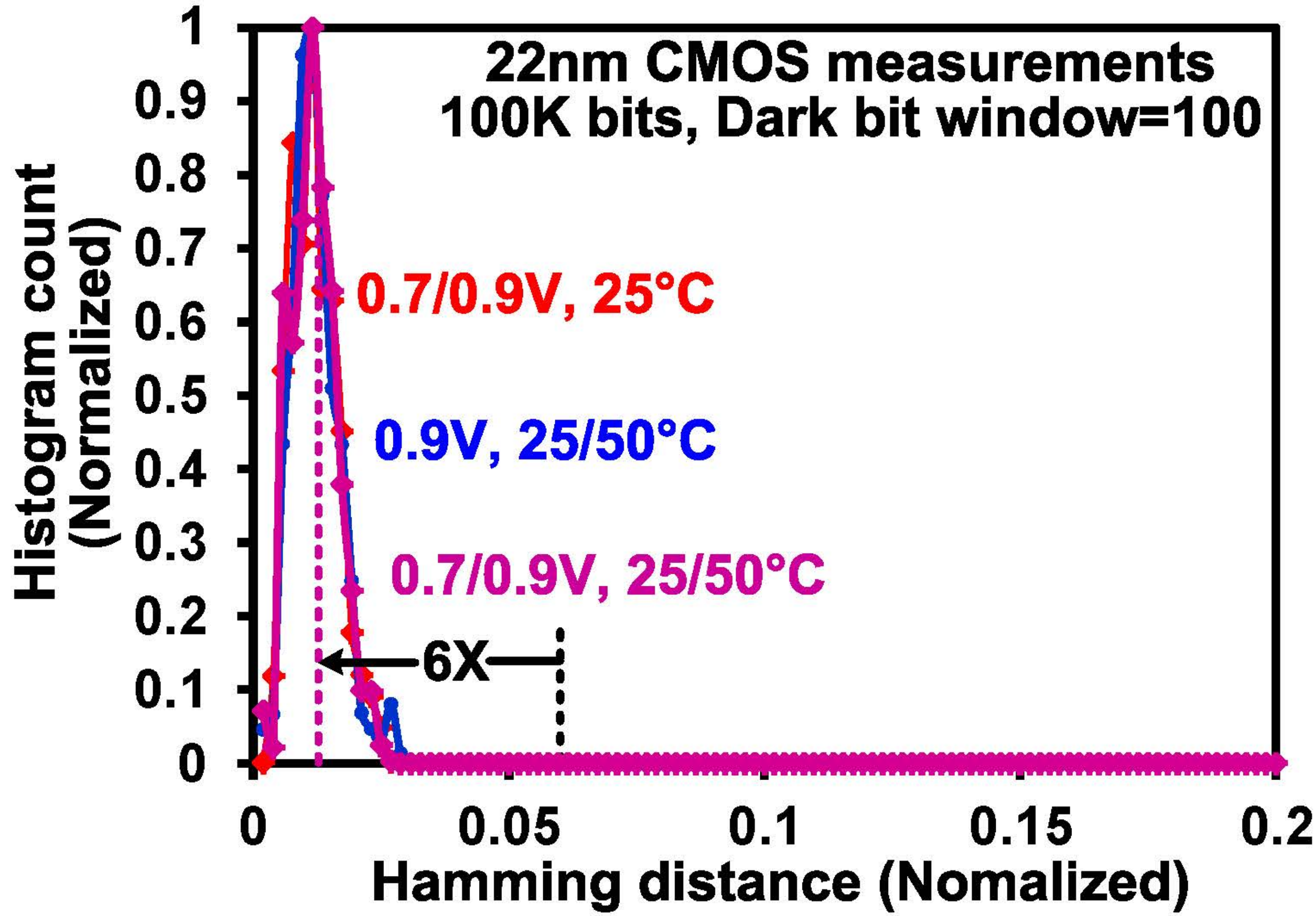
- Intra-PUF distance: temporal correlation within PUF bit
- Inter-PUF distance: in-die and die-to-die correlation
- 19X separation between inter/intra Hamming distance

Effect of Voltage/Temp Variations



- Voltage and temperature shifts ⇒ 1.8X↑ intra-PUF distance
- Temperature variation causes systematic shift in PUF bias
- Maximum bit-error rate increases by 40%

Variation Tolerance With Dark Bits



- 100 cycle dark bit window eliminates bits with high sensitivity to voltage/temperature variation
- Average intra-PUF distance reduces to 0.01 (6X ↓)

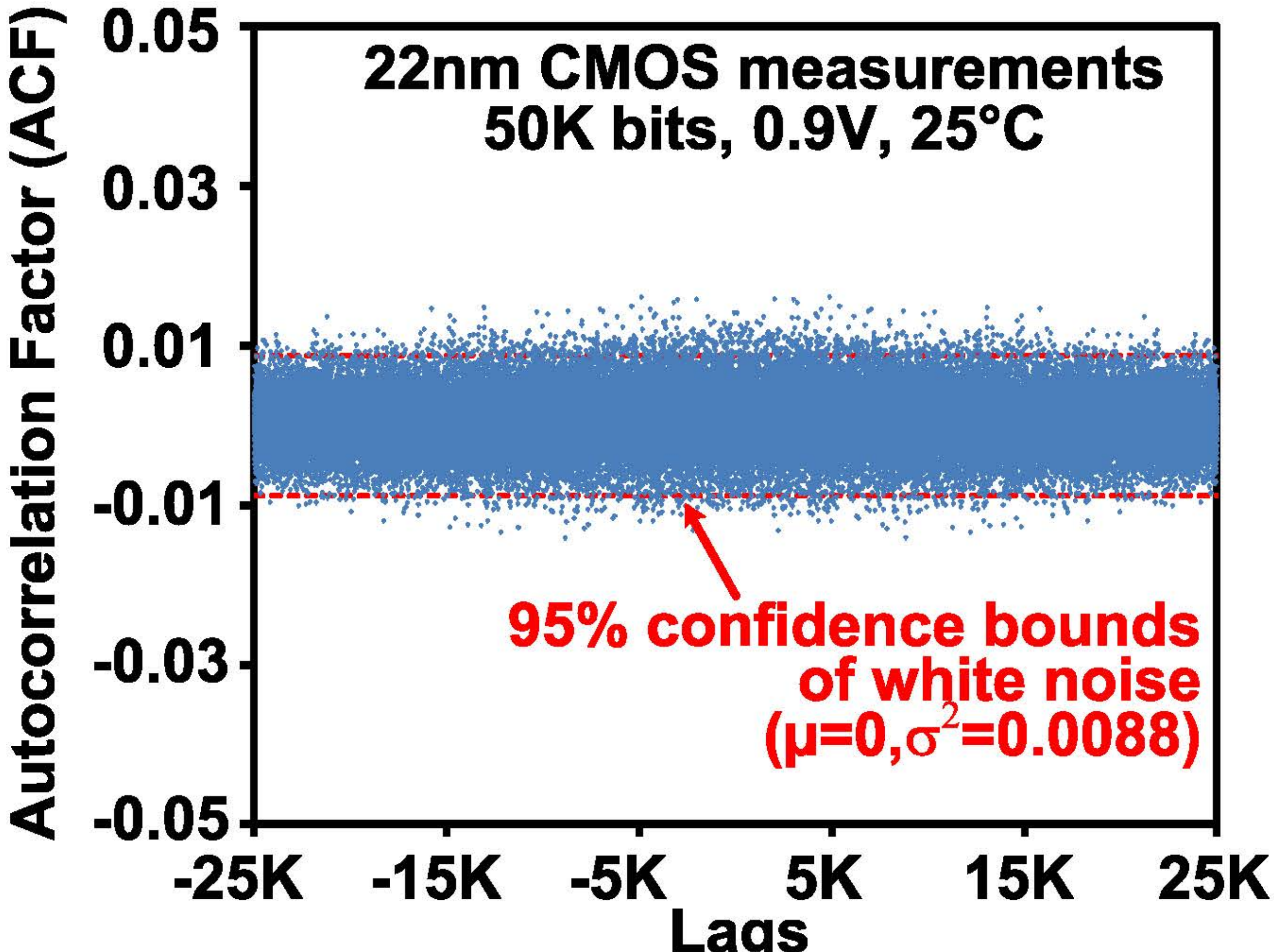
NIST Randomness Tests

22nm CMOS measurements, 0.9V, 25°C

Test name	Stream length	No of runs	Pass %	Average P-value	Pass?
Frequency	1000	45	93	0.0006	YES
Block frequency	1000	45	100	0.1315	YES
Runs	1000	45	98	0.1996	YES
Longest run of ones	1000	45	100	0.1516	YES
Cumulative sums	1000	45	93	0.0231	YES
Rank	45000	1	100	0.6707	YES
FFT	1000	45	98	0.0001	YES
Non-overlapping template matching	1000(m = 5)	45	100	0.0914	YES
Serial	1000 (m = 4)	45	98	0.0164	YES
Approximate entropy	1000 (m = 4)	45	98	0.8942	YES

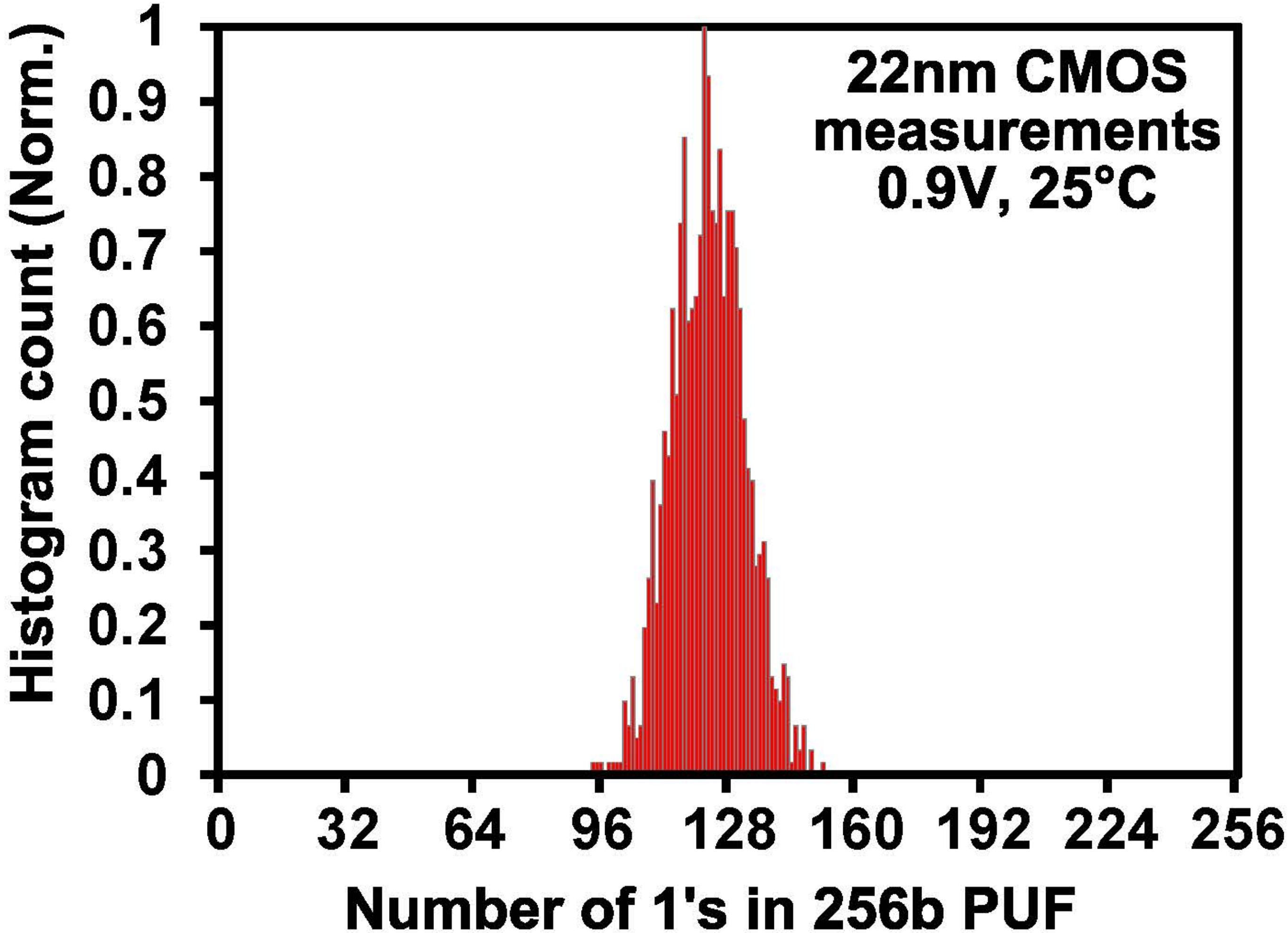
- Passes NIST randomness tests
- No periodicity or patterns detected in PUF key
- Measured entropy = 0.9997

Auto-correlation Tests



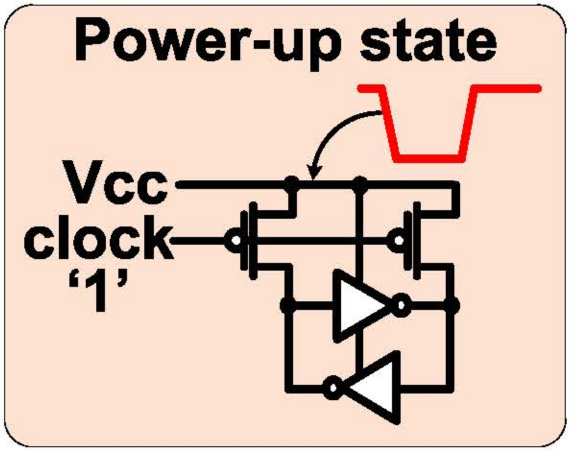
- Correlation against shifted version of PUF bitstream
- ACFs within 95% confidence bounds of ideal Gaussian
- Bitstream displays no spatial correlation across the die

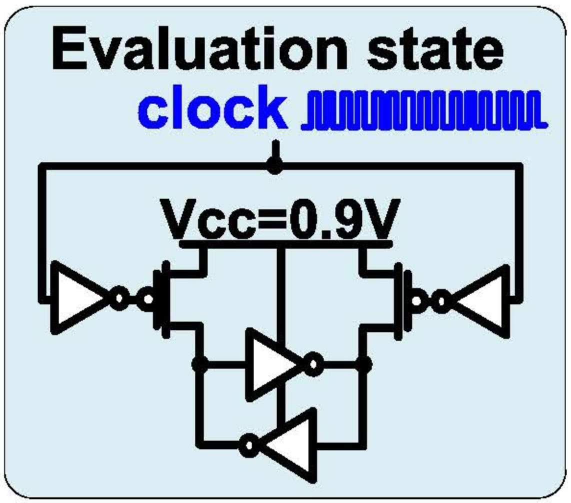
Distribution of 1's in PUF Key

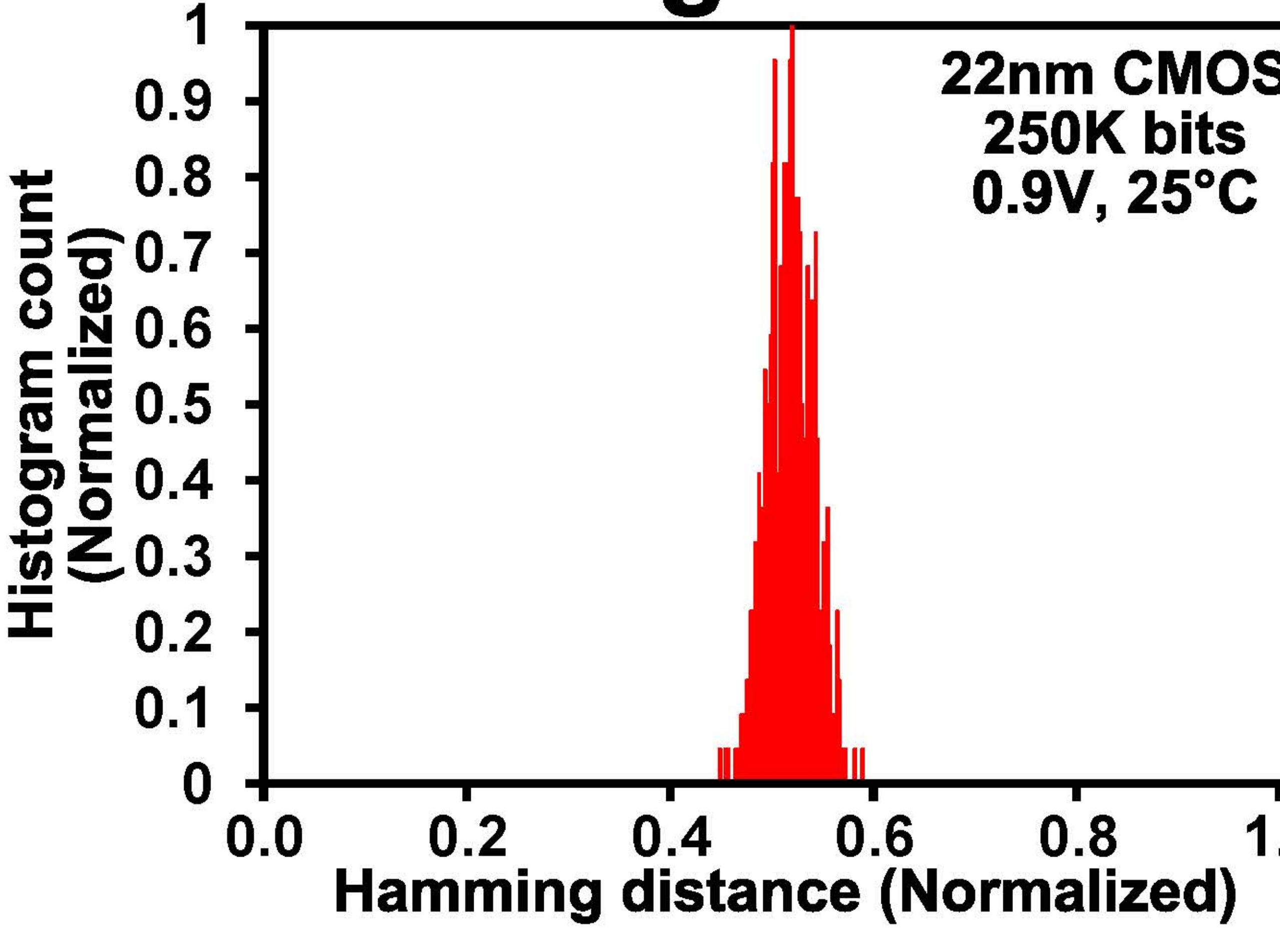


- Tests 0/1 bias & correlation among adjacent bits
- Random distribution of 1's in PUF word with μ=123,σ=9

Tolerance to Probing Attacks



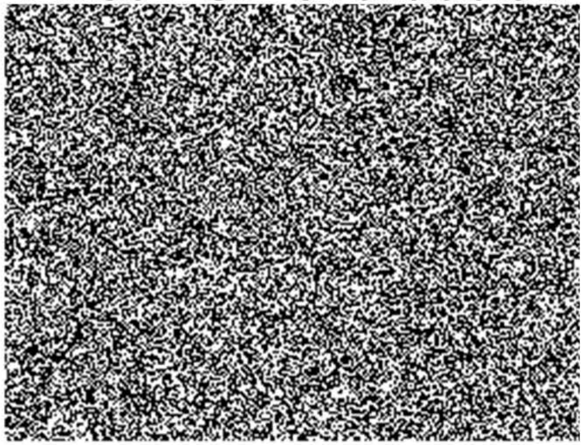




- Power-up state: vulnerable to invasive probing attacks
- Evaluation state: influenced by clock transients
- 51% of PUF evaluation states differ from power-up value
  ⇒2X higher immunity to probing attacks

Measurement Summary

First PUF evaluation

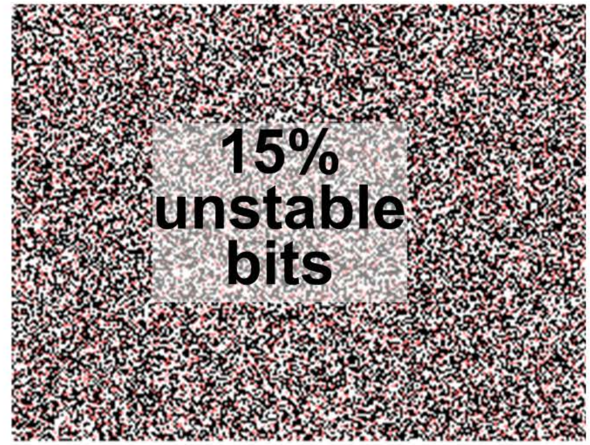


■:0 □:1

Raw PUF

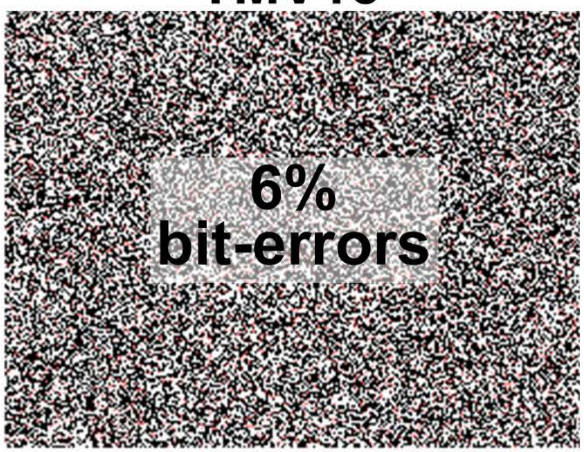
■:Unstable

TMV15



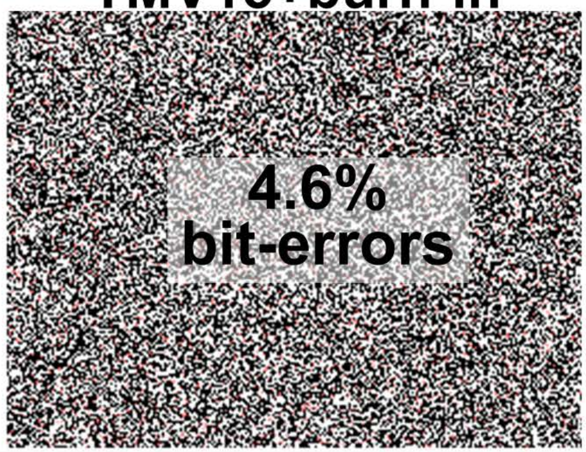
■:Unstable

TMV15

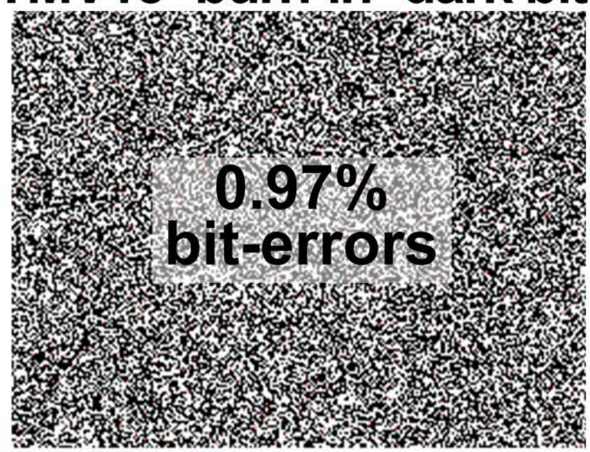


■:Bit-error

TMV15+burn-in



TMV15+burn-in+dark bits



■:Bit-error

22nm CMOS, 0.9V, 25°C

Total power @ 2GHz	25µW/bit
Leakage power	1.4µW/bit
PUF energy	13fJ/bit
TMV15 energy	0.19pJ/bit

Summary

- 0.19pJ/bit, 2GHz variation-tolerant hybrid PUF circuit in 22nm tri-gate CMOS
- PUF stabilization techniques:
  - Temporal-majority voting circuit (32% ↓)
  - Burn-in hardening (22% ↓)
  - Soft dark bits (78% ↓)
- 19X separation between intra/inter-PUF Hamming
- Passes NIST tests with entropy=0.9997
- 2X higher immunity to invasive probing attacks

A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS

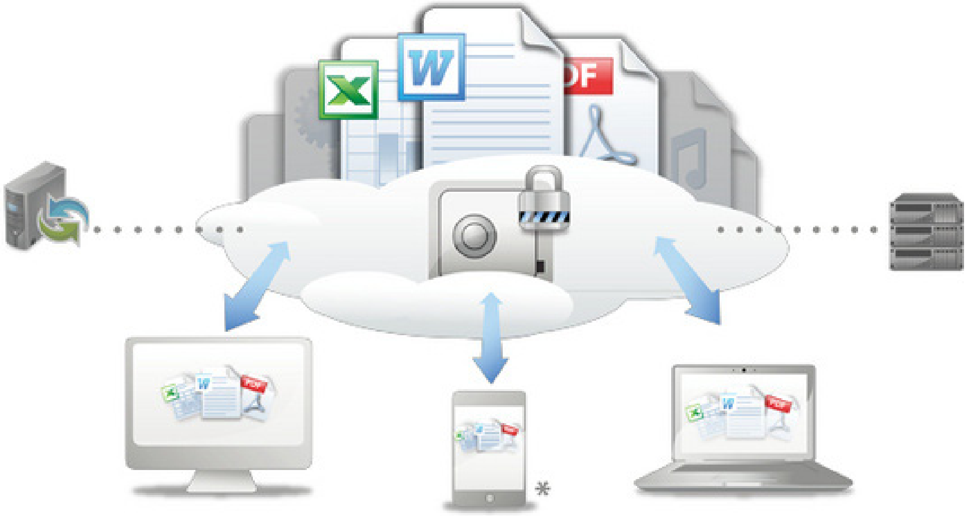
Kaiyuan Yang, David Fick, Michael B. Henry,
Yoonmyung Lee, David Blaauw, Dennis Sylvester

University of Michigan, Ann Arbor

Motivation

- **True Random Number Generator (TRNG)**
  - Independent and unpredictable bits
- **Applications**
  - Encryption
  - Numerical methods
  - Stochastic computing

Source: accpc.com



Source: storagenewsletter.com

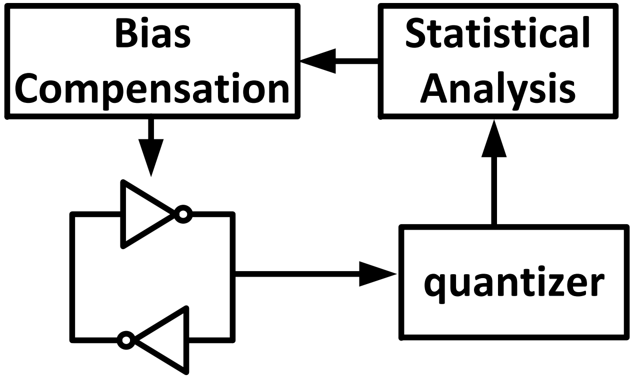
Source: eecs.umich.edu

Prior Art

- **Direct amplification of noise**
  - Resistor thermal noise (C. Petrie, TCAS-I, 2000)
  - Oxide-trap noise (R. Brederlow, ISSCC, 2006)
  - SiN FET noise (M. Matsumoto, ISSCC, 2008)

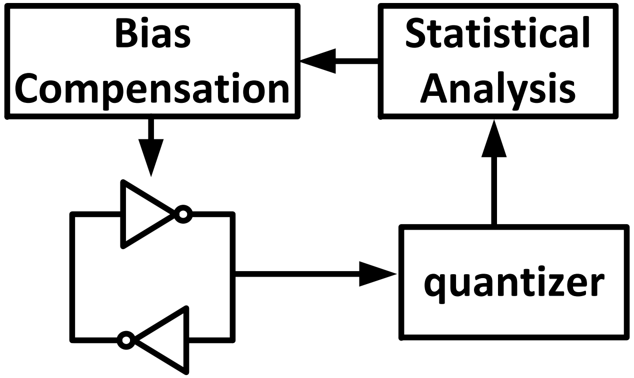
Prior Art

- **Direct amplification of noise**
  - Resistor thermal noise (C. Petrie, TCAS-I, 2000)
  - Oxide-trap noise (R. Brederlow, ISSCC, 2006)
  - SiN FET noise (M. Matsumoto, ISSCC, 2008)
- **Metastability** (C. Tokunaga, ISSCC, 2007; S. Mathew, JSSC, 2012)
  - High speed
  - Complexity in runtime calibration



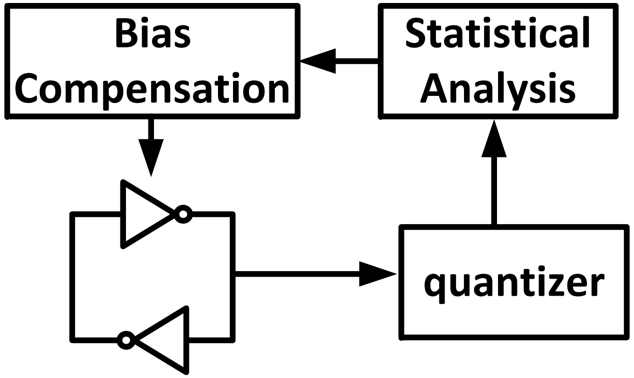
Prior Art

- **Direct amplification of noise**
  - Resistor thermal noise (C. Petrie, TCAS-I, 2000)
  - Oxide-trap noise (R. Brederlow, ISSCC, 2006)
  - SiN FET noise (M. Matsumoto, ISSCC, 2008)
- **Metastability** (C. Tokunaga, ISSCC, 2007; S. Mathew, JSSC, 2012)
  - High speed
  - Complexity in runtime calibration
- **Time to oxide breakdown** (N. Liu, VLSIC, 2010)
  - High randomness
  - Low power efficiency and limited lifetime

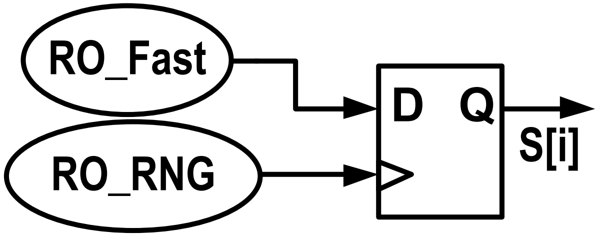


Prior Art

- **Direct amplification of noise**
  - Resistor thermal noise (C. Petrie, TCAS-I, 2000)
  - Oxide-trap noise (R. Brederlow, ISSCC, 2006)
  - SiN FET noise (M. Matsumoto, ISSCC, 2008)
- **Metastability** (C. Tokunaga, ISSCC, 2007; S. Mathew, JSSC, 2012)
  - High speed
  - Complexity in runtime calibration

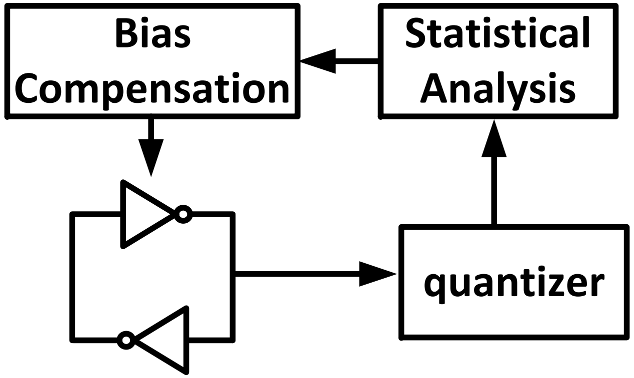


- **Time to oxide breakdown** (N. Liu, VLSIC, 2010)
  - High randomness
  - Low power efficiency and limited lifetime
- **Jitter in oscillators**
  (M. Bucci, Trans. Computers, 2003; M. Bucci, TCAS-I, 2008)
  - All digital, high speed, compact design
  - Limited entropy

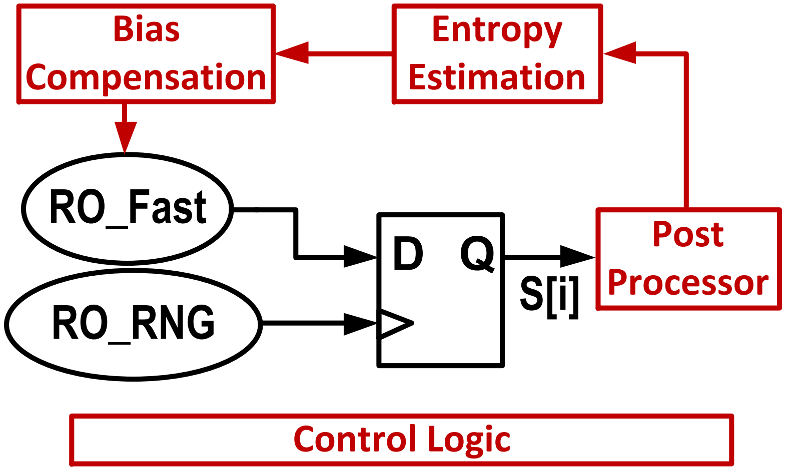


Prior Art

- **Direct amplification of noise**
  - Resistor thermal noise (C. Petrie, TCAS-I, 2000)
  - Oxide-trap noise (R. Brederlow, ISSCC, 2006)
  - SiN FET noise (M. Matsumoto, ISSCC, 2008)
- **Metastability** (C. Tokunaga, ISSCC, 2007; S. Mathew, JSSC, 2012)
  - High speed
  - Complexity in runtime calibration

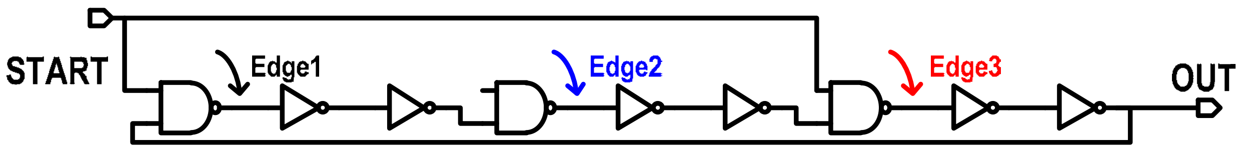


- **Time to oxide breakdown** (N. Liu, VLSIC, 2010)
  - High randomness
  - Low power efficiency and limited lifetime
- **Jitter in oscillators**
  (M. Bucci, Trans. Computers, 2003; M. Bucci, TCAS-I, 2008)
  - All digital, high speed, compact design
  - Limited entropy
  - Extra design effort, power and area overhead



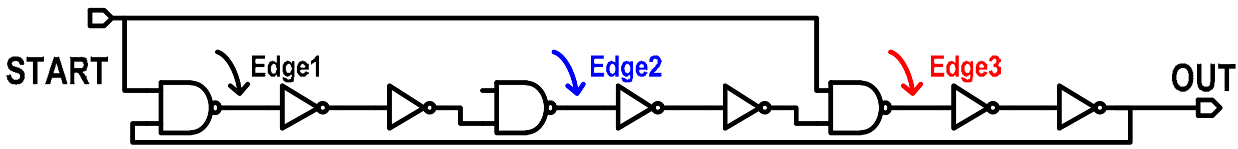
Proposed TRNG

- **Entropy source**
  - Time for a 3 edge oscillation mode (3x frequency) to collapse to normal mode (1x frequency)



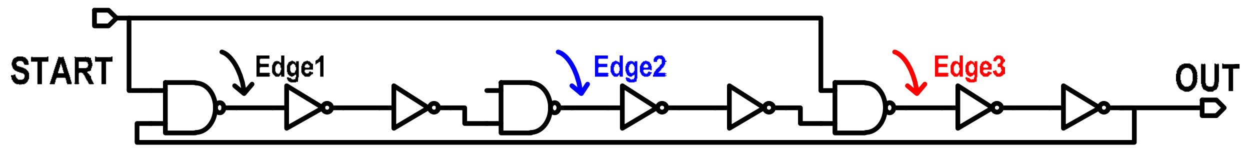
Proposed TRNG

- **Entropy source**
  - Time for a 3 edge oscillation mode (3x frequency) to collapse to normal mode (1x frequency)
- **Ease of design**
  - Design portability
  - Fully synthesized with only standard cells
  - Commercial APR tools



Proposed TRNG

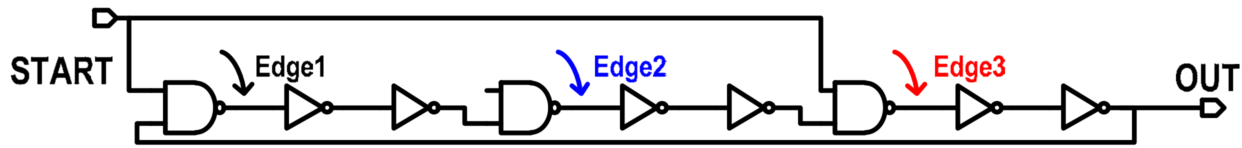
- **Entropy source**
  - Time for a 3 edge oscillation mode (3x frequency) to collapse to normal mode (1x frequency)



- **Ease of design**
  - Design portability
  - Fully synthesized with only standard cells
  - Commercial APR tools
- **Small area & high energy efficiency**
  - Cost efficiency
  - Critical for tiny systems

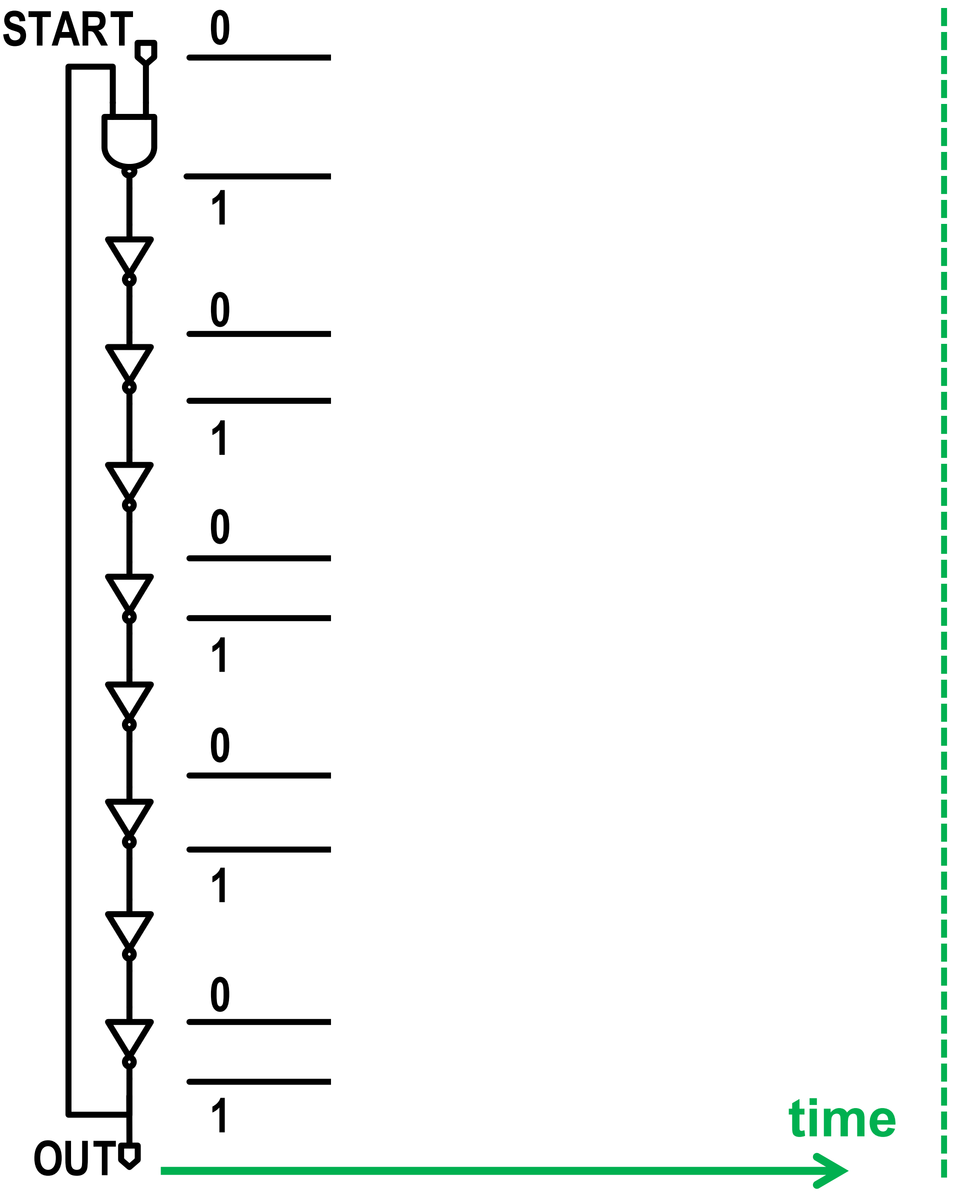
Proposed TRNG

- **Entropy source**
  - Time for a 3 edge oscillation mode (3x frequency) to collapse to normal mode (1x frequency)

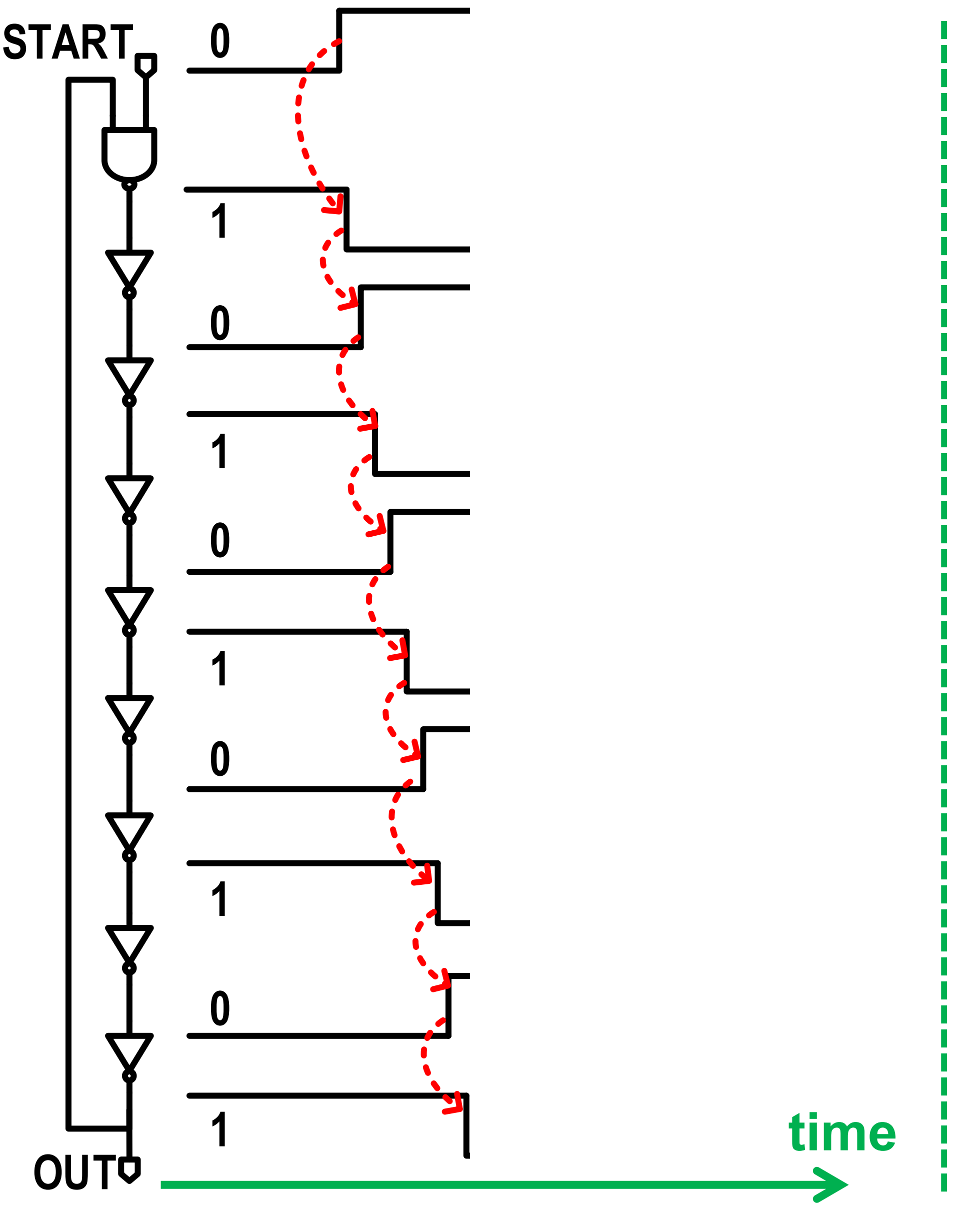


- **Ease of design**
  - Design portability
  - Fully synthesized with only standard cells
  - Commercial APR tools
- **Small area & high energy efficiency**
  - Cost efficiency
  - Critical for tiny systems
- **Attack resistance**
  - Deliberate attack
  - Environmental noise

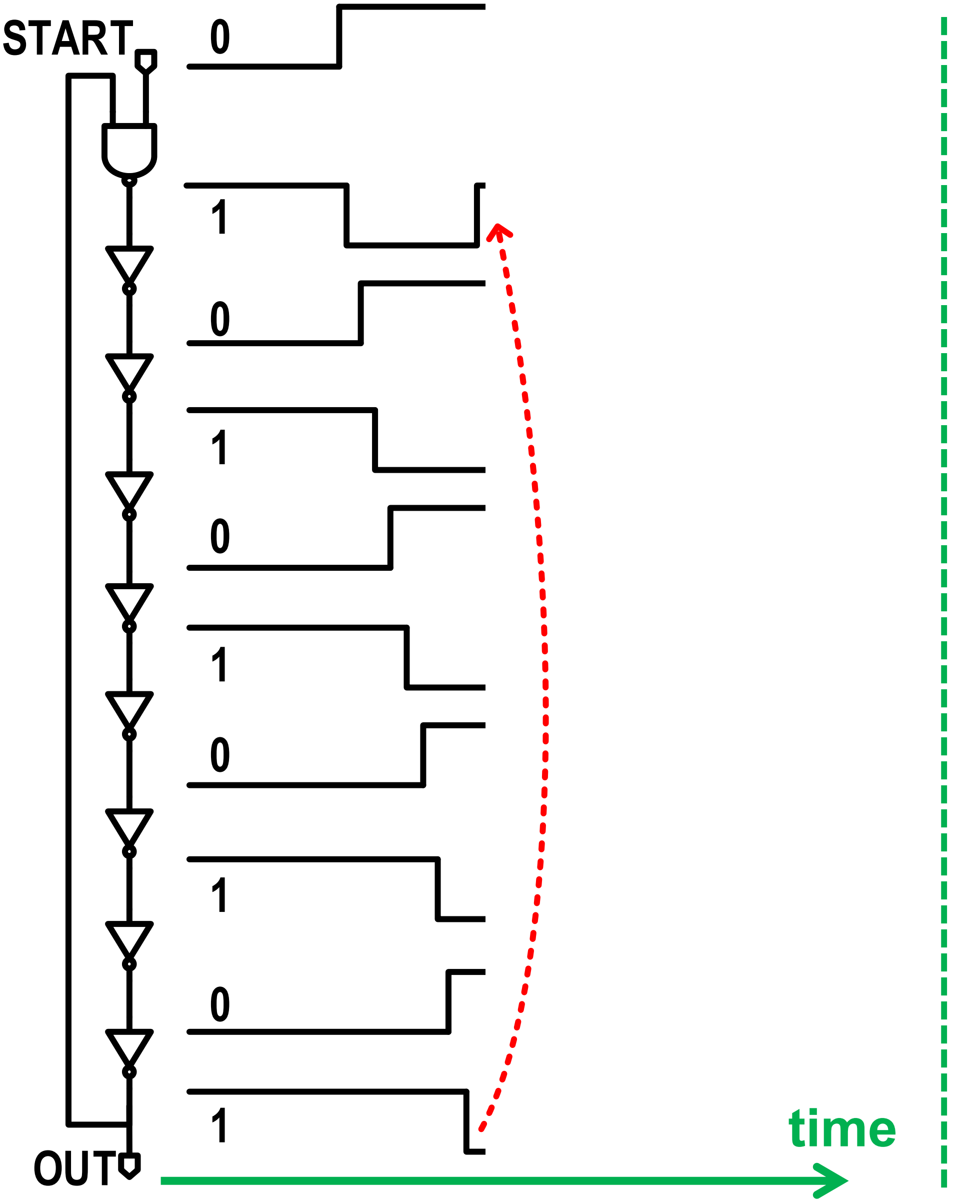
Single-Edge Oscillator



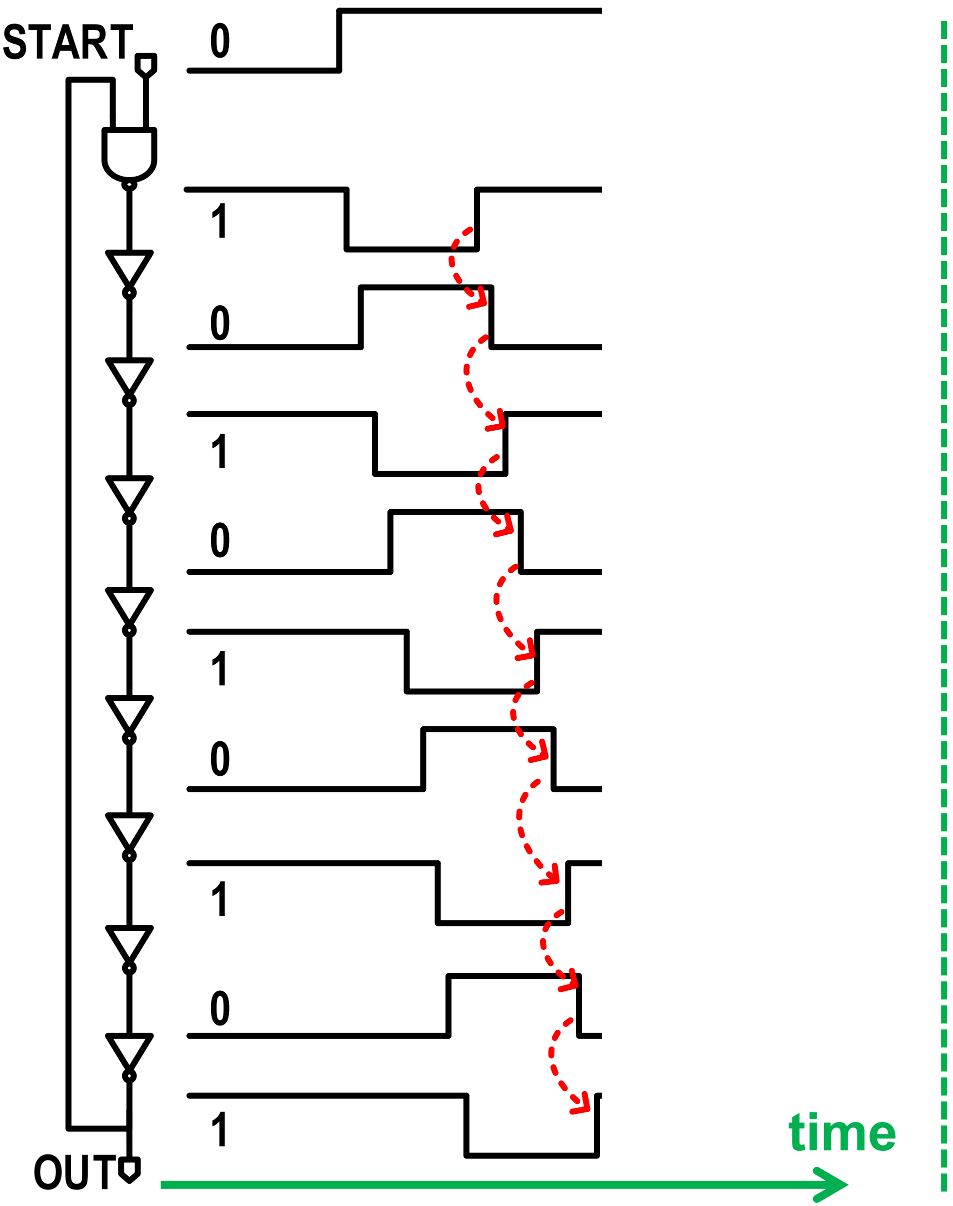
Single-Edge Oscillator



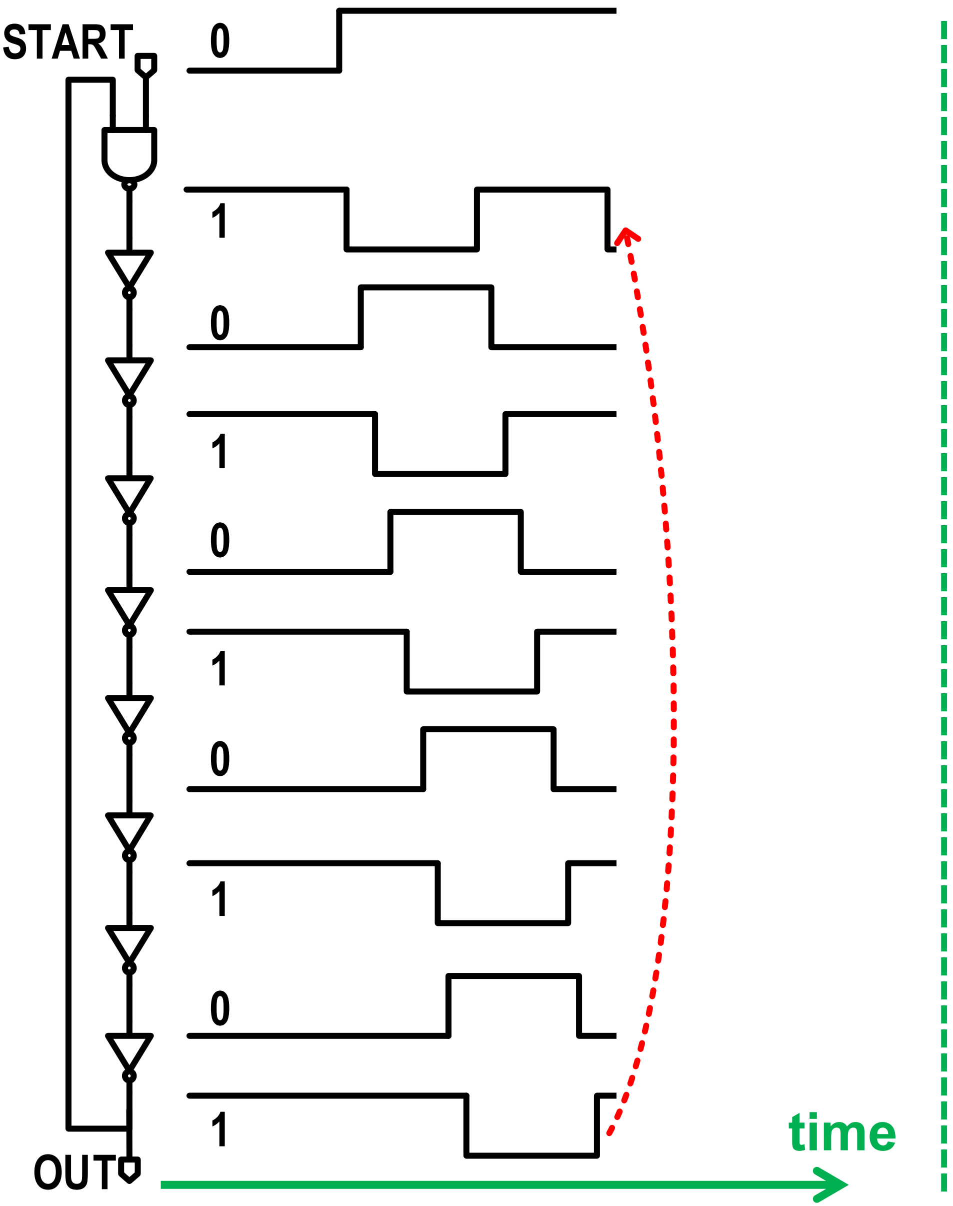
Single-Edge Oscillator



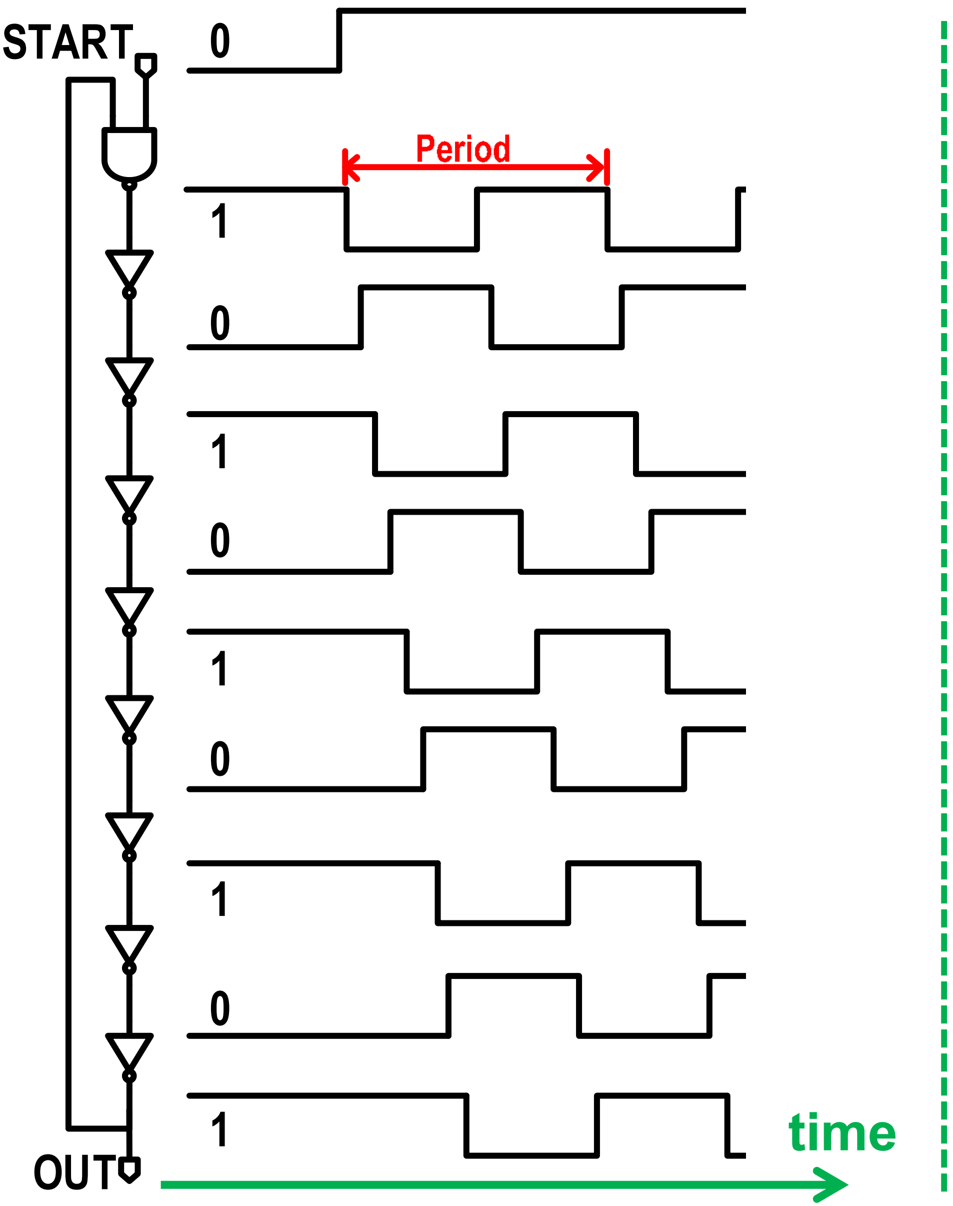
Single-Edge Oscillator



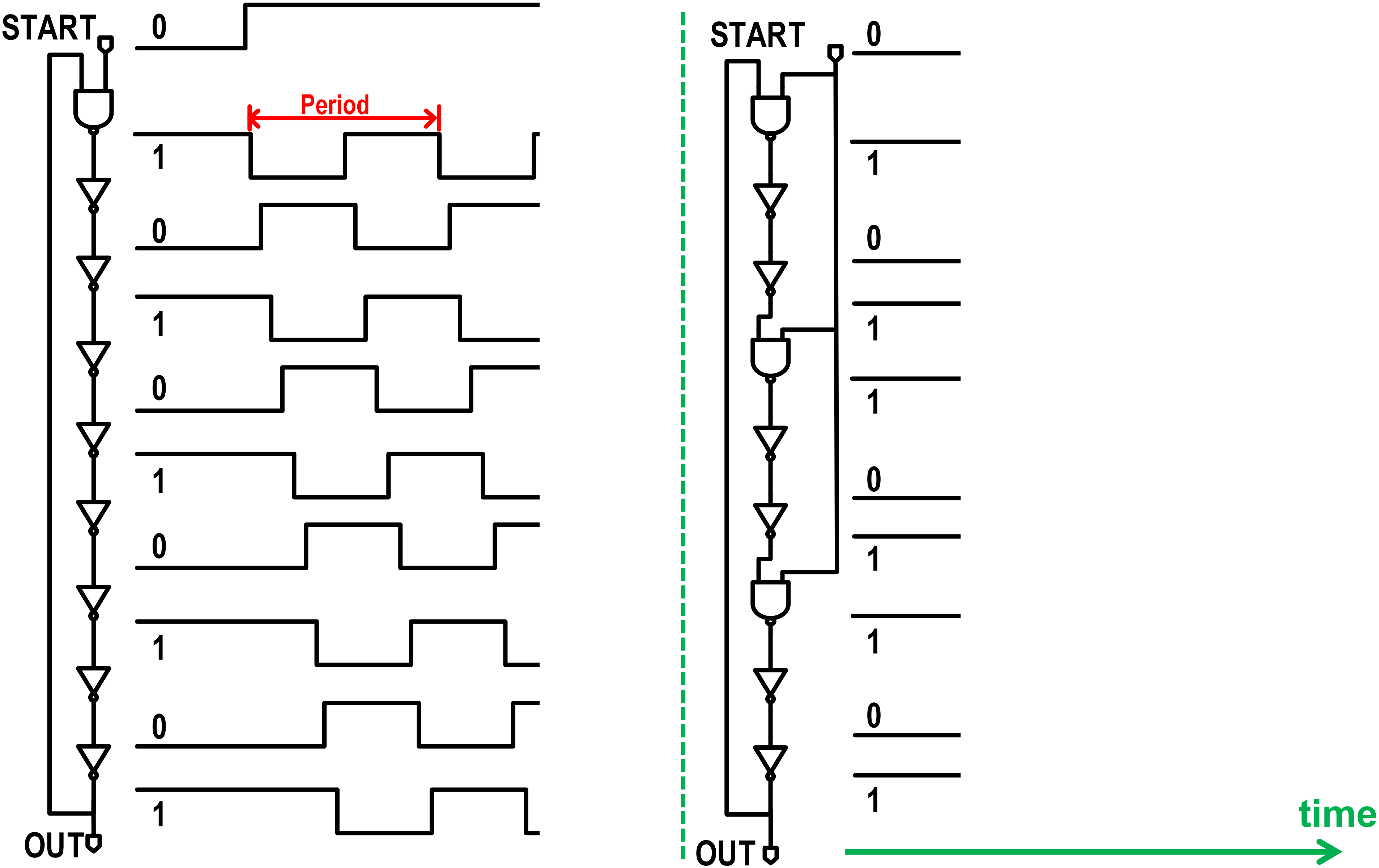
Single-Edge Oscillator



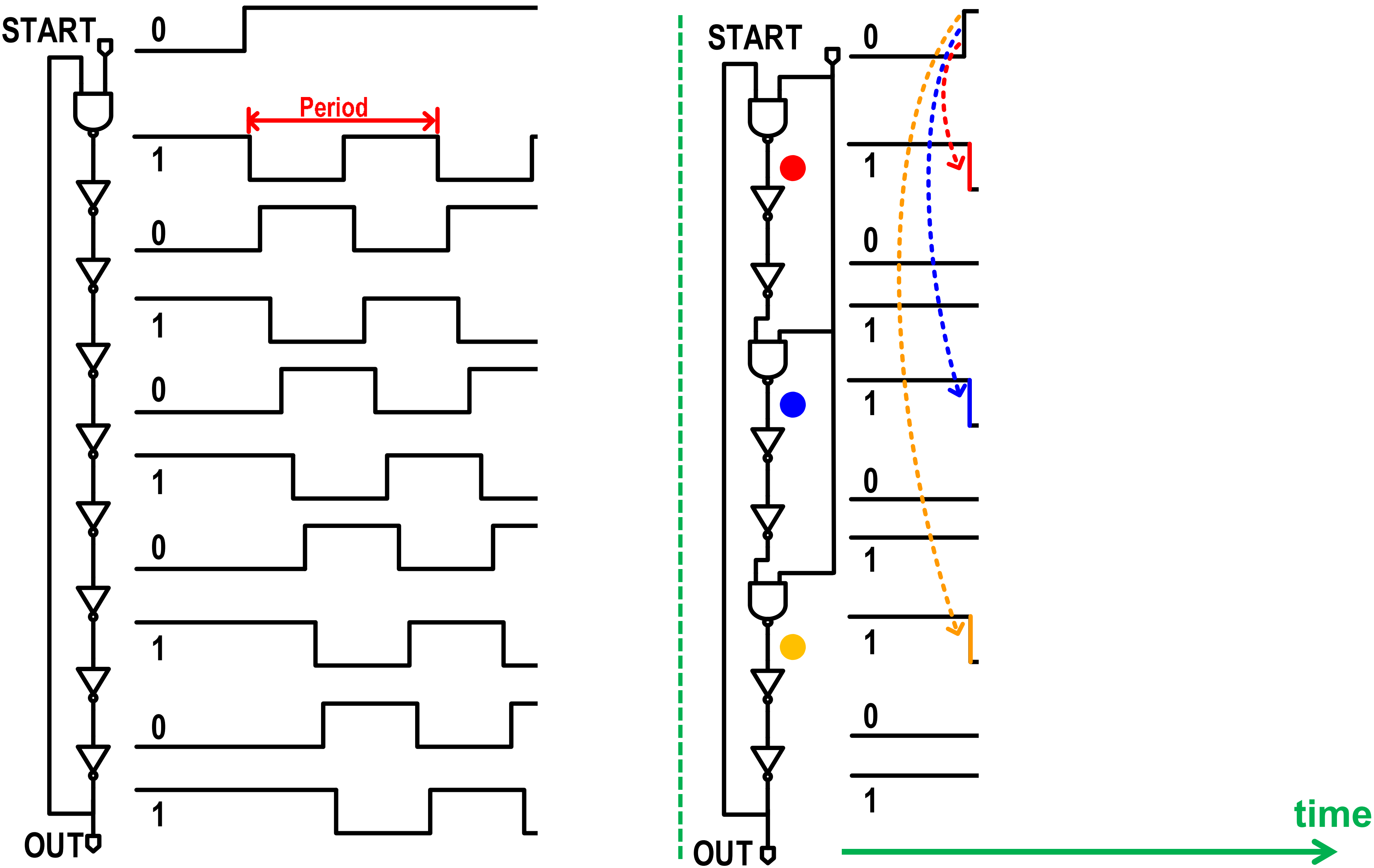
Single-Edge Oscillator



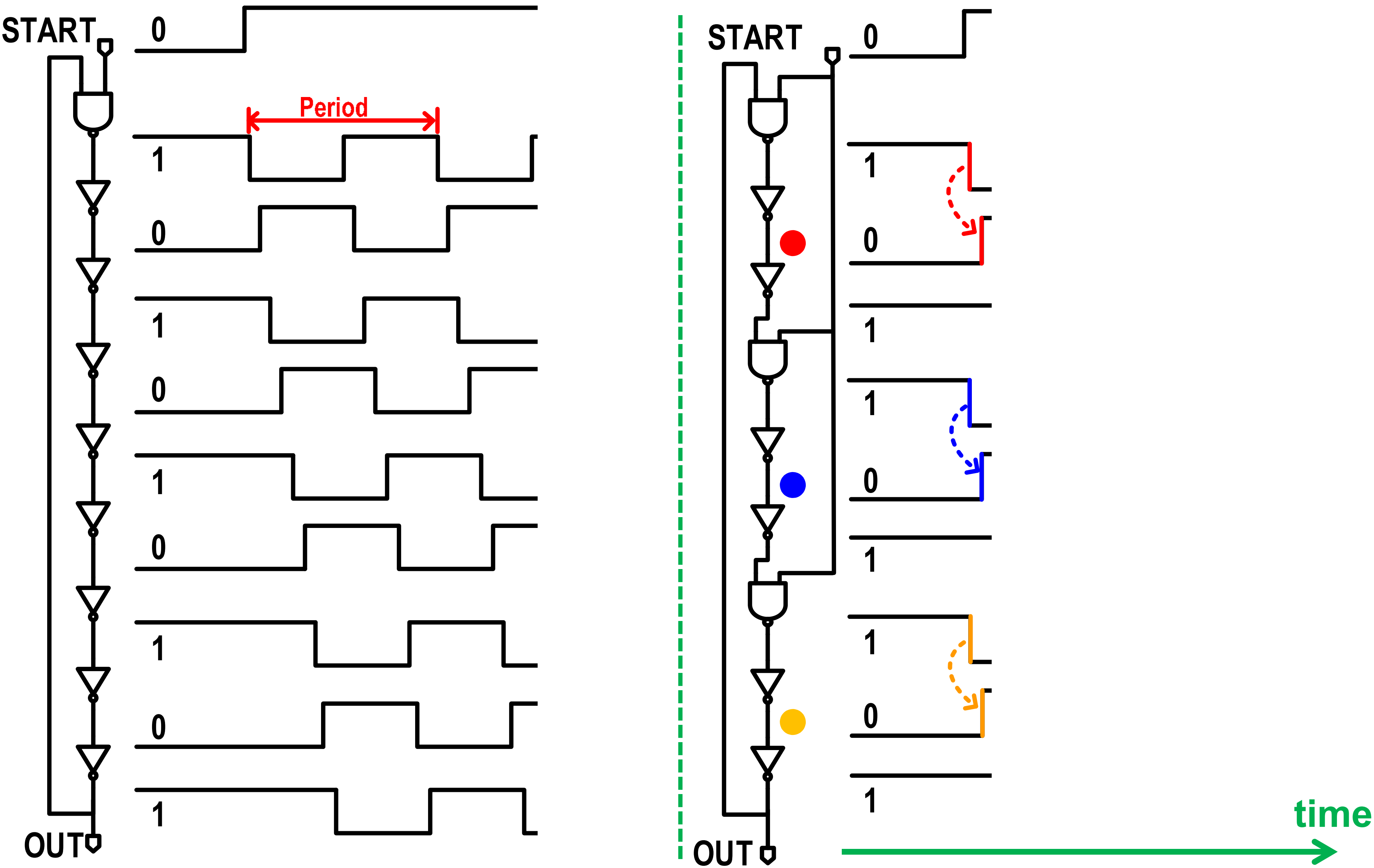
Multi-Mode Oscillator



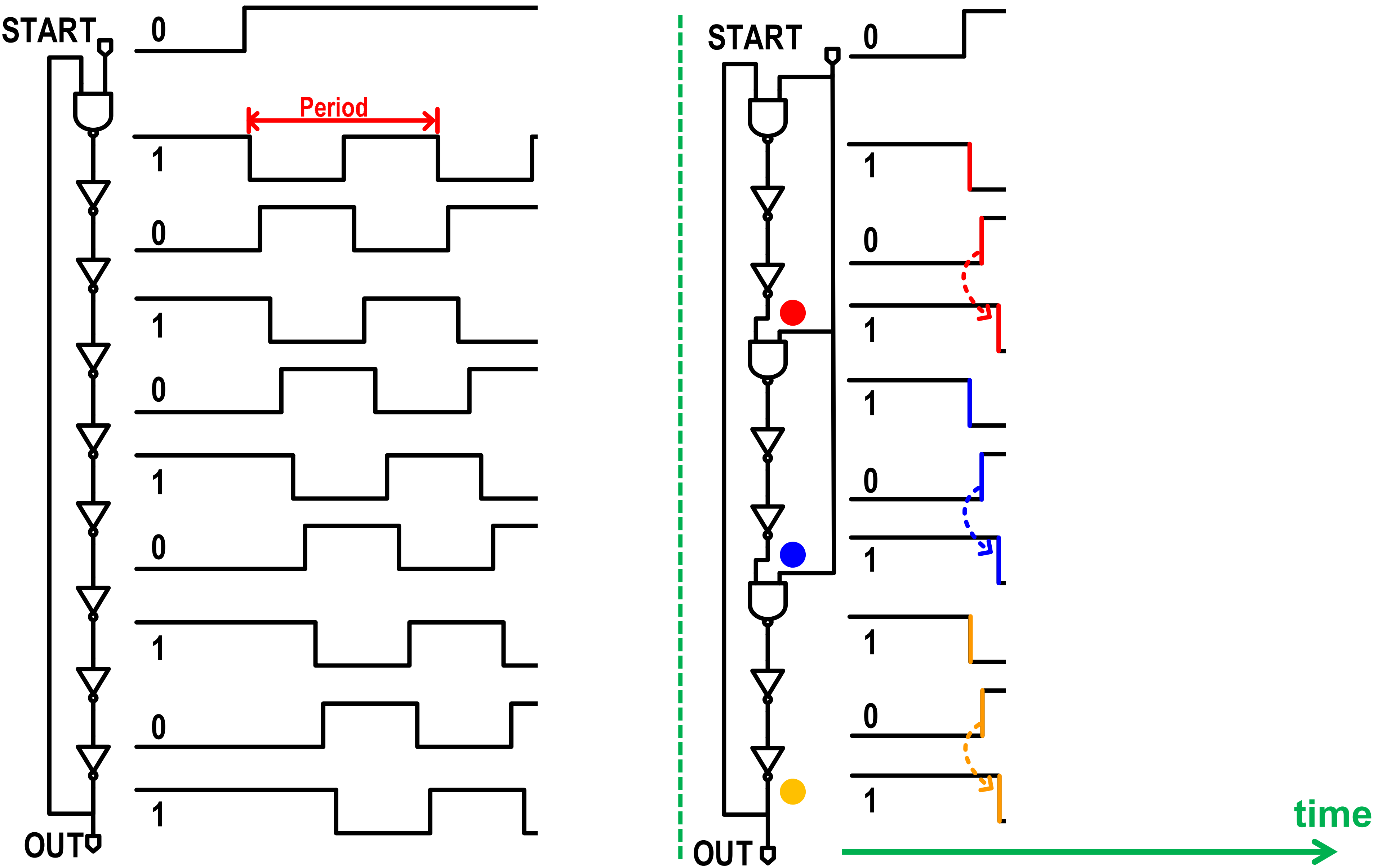
Multi-Mode Oscillator



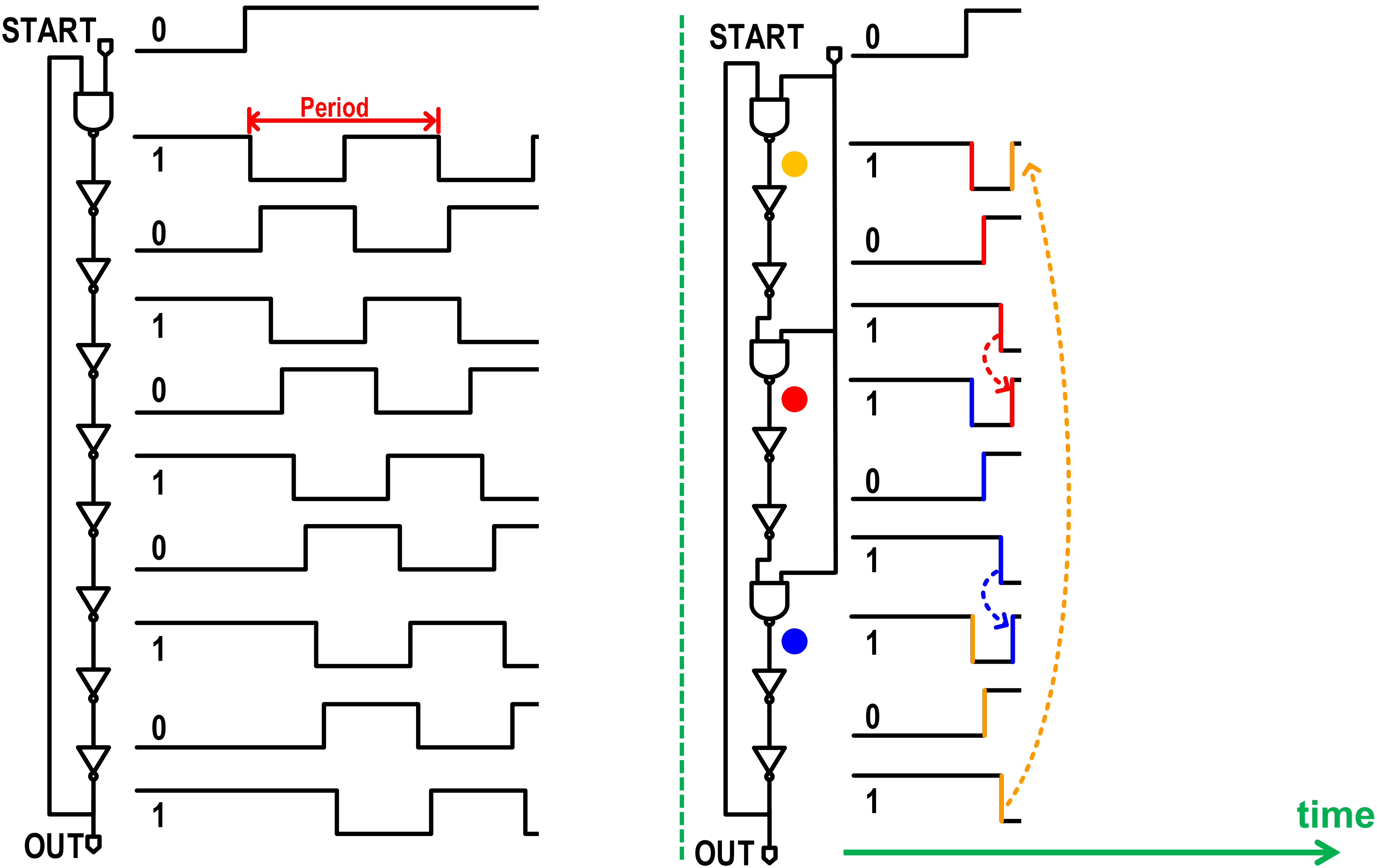
Multi-Mode Oscillator



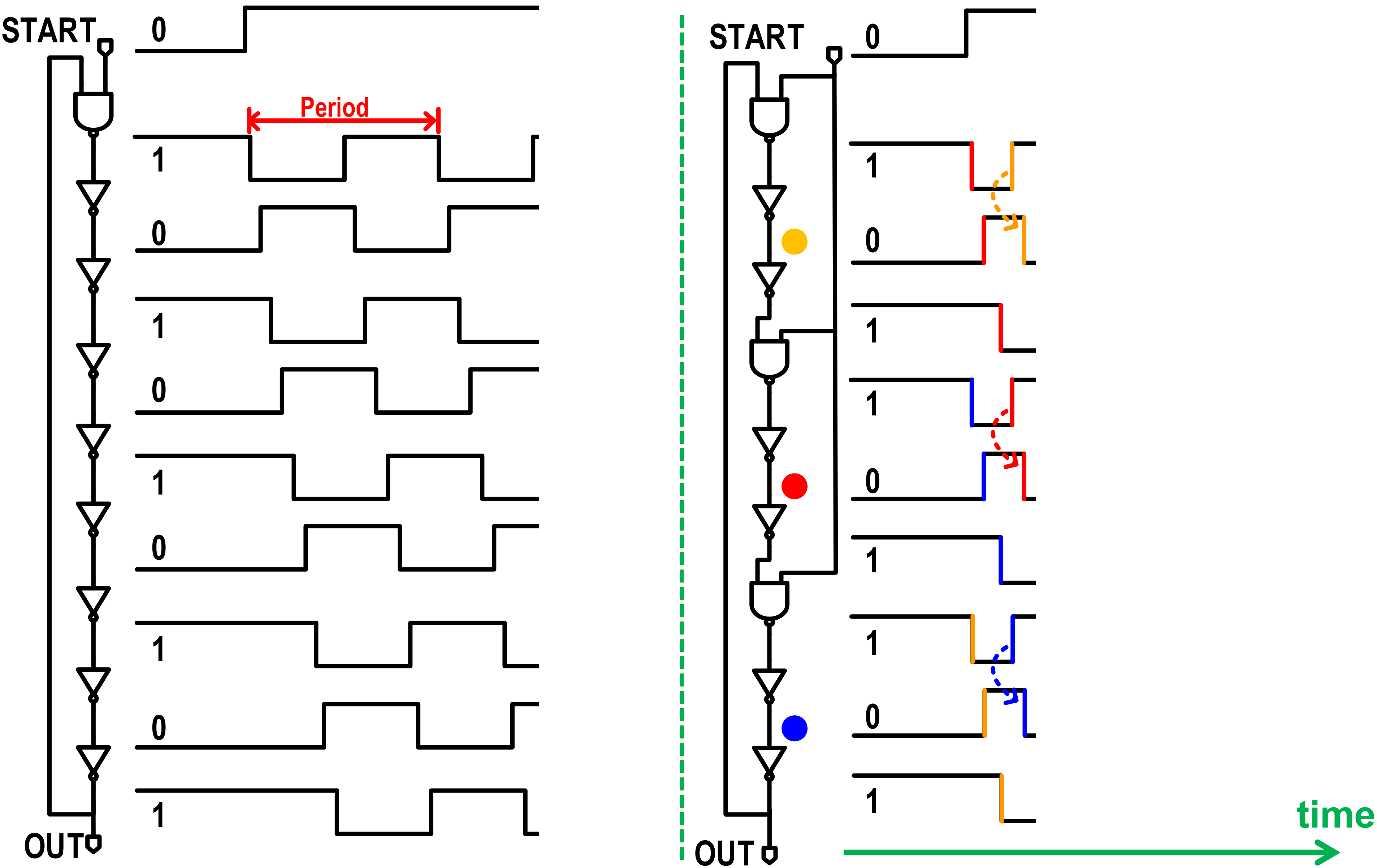
Multi-Mode Oscillator



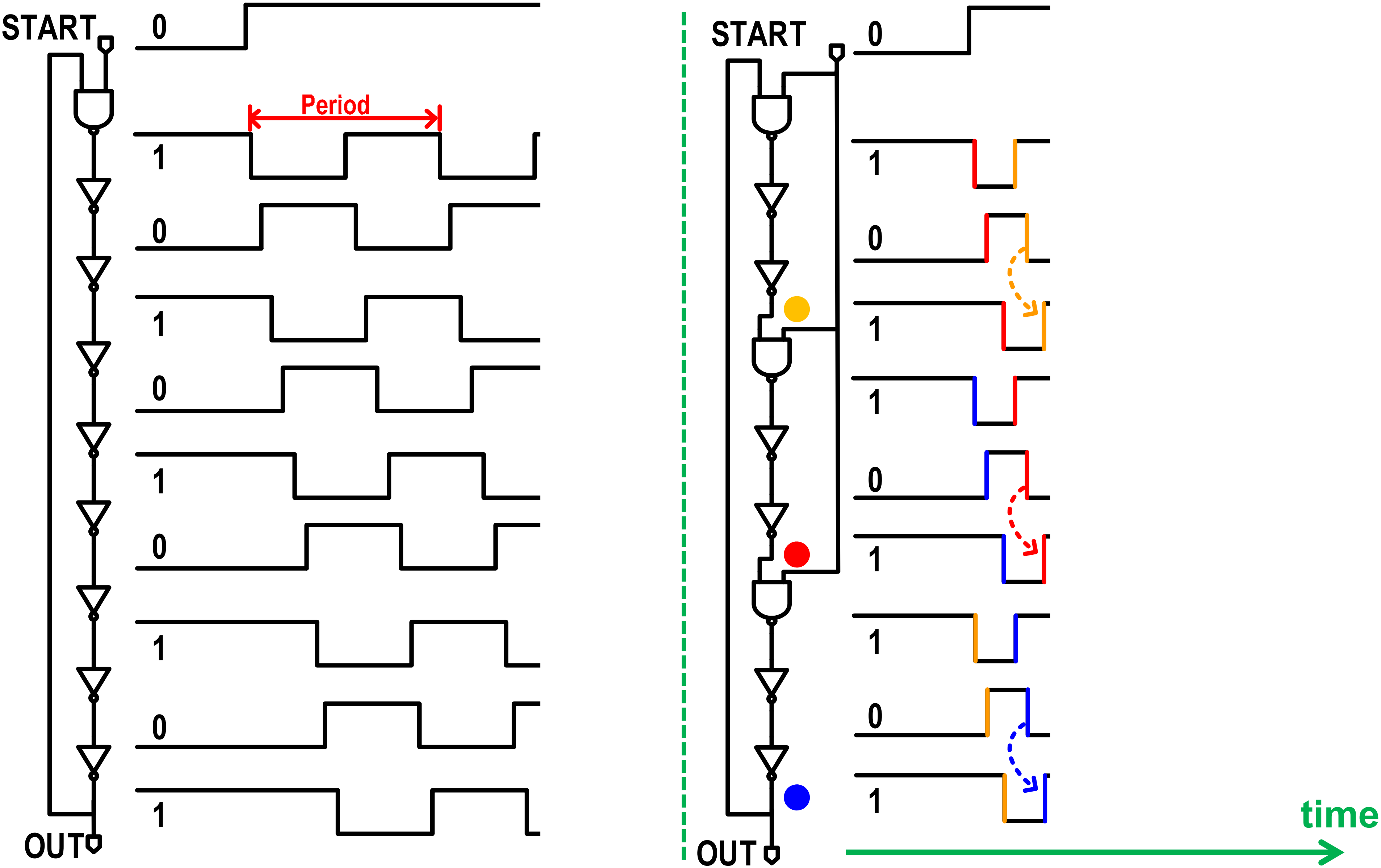
Multi-Mode Oscillator



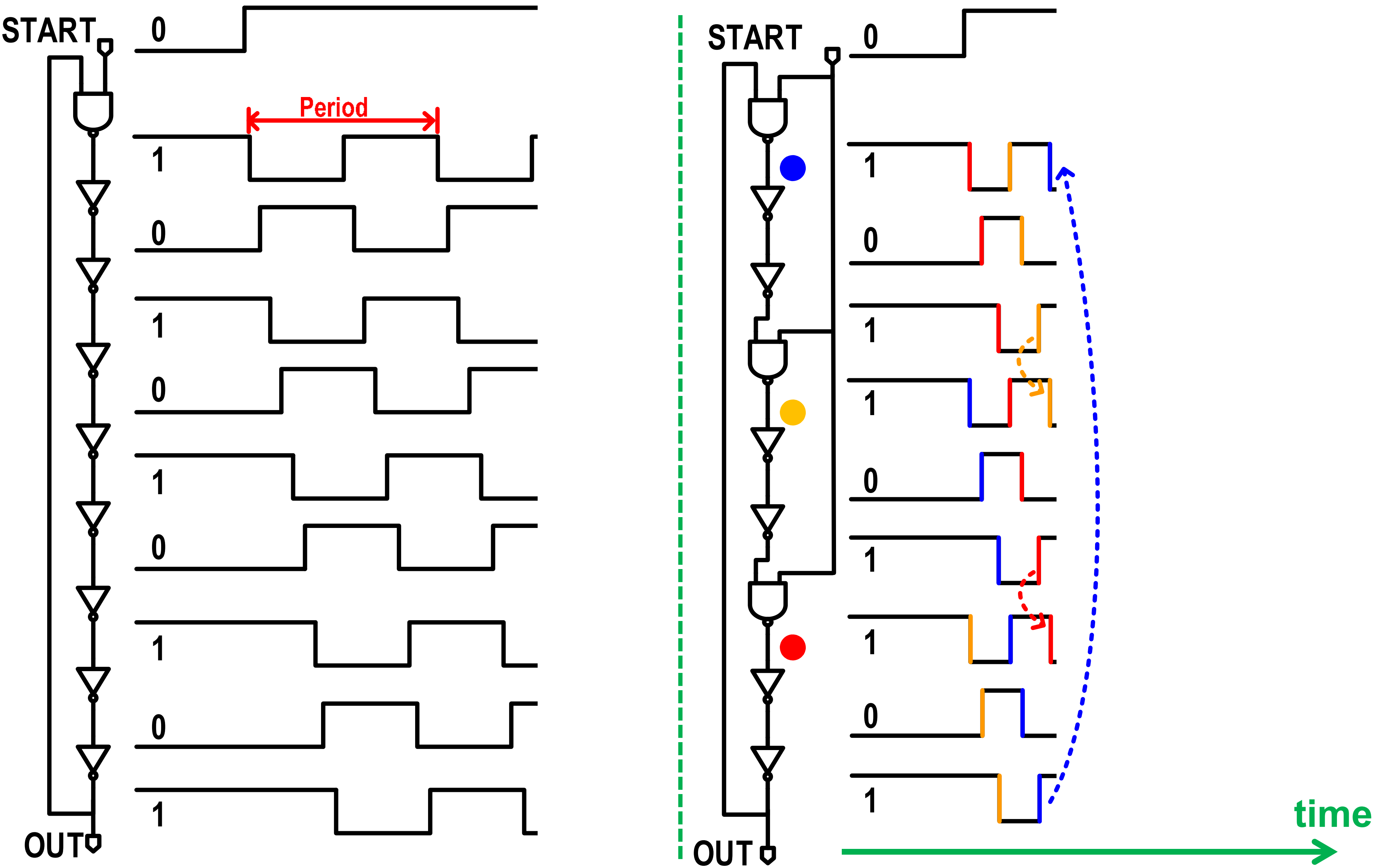
Multi-Mode Oscillator



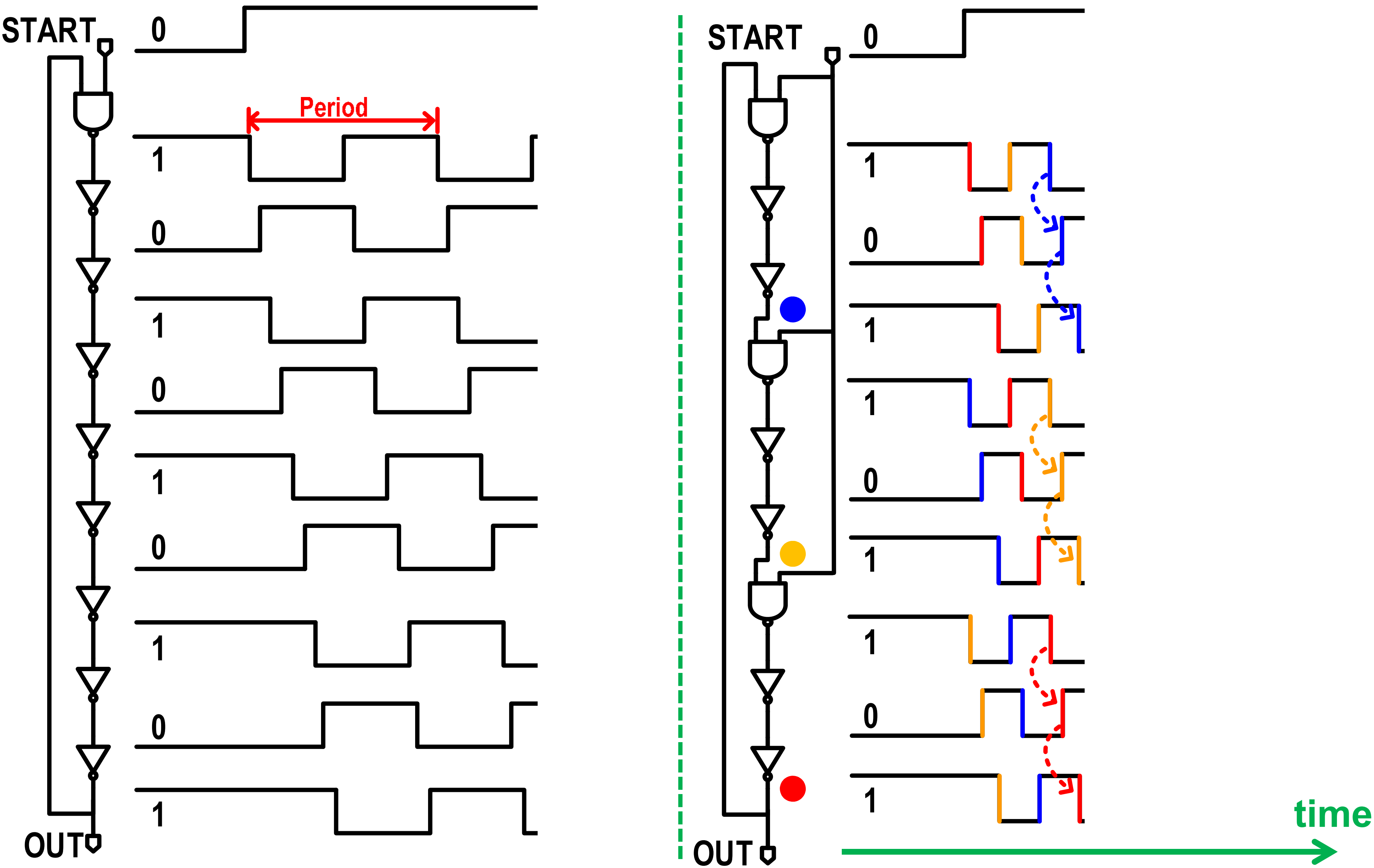
Multi-Mode Oscillator



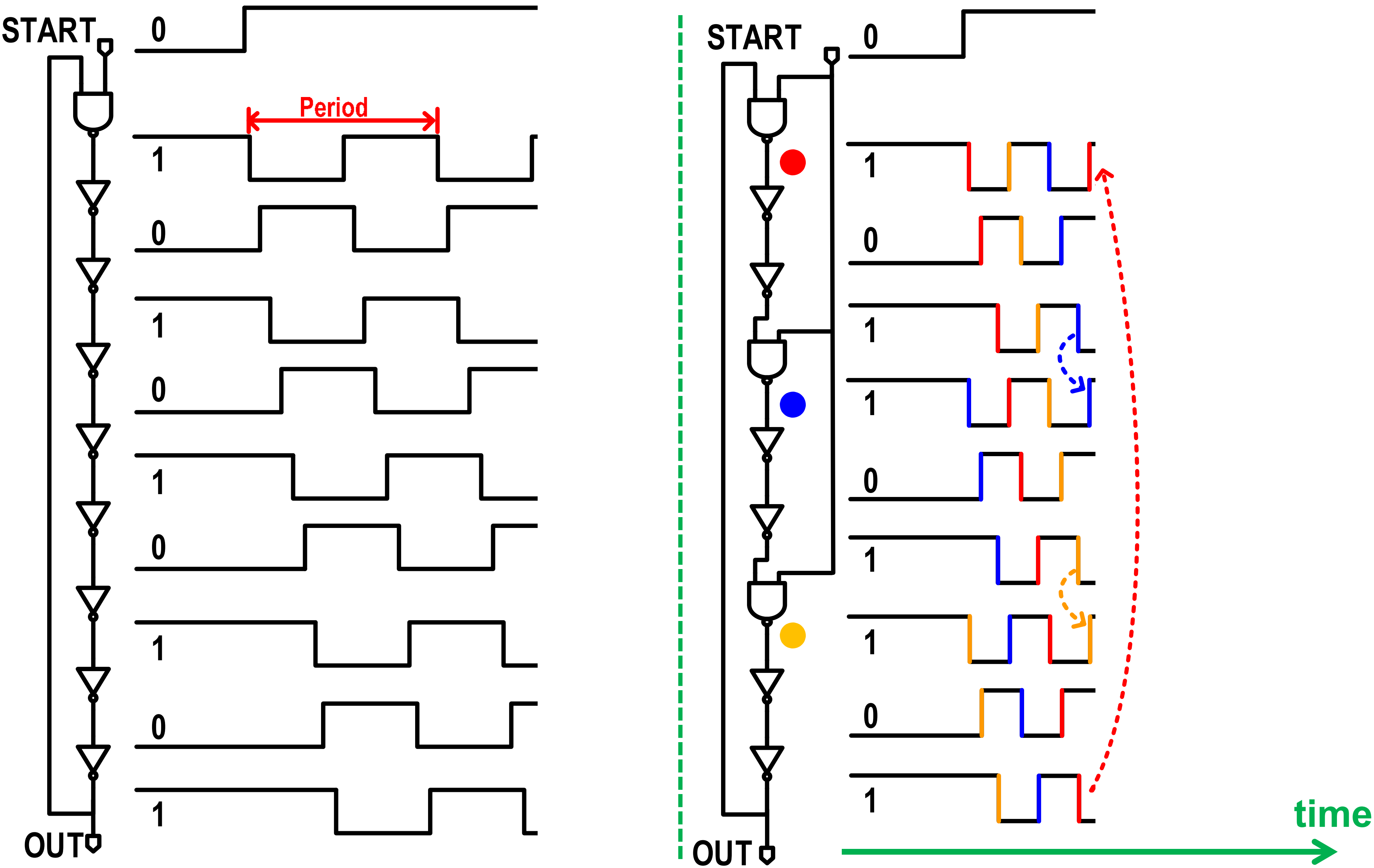
Multi-Mode Oscillator



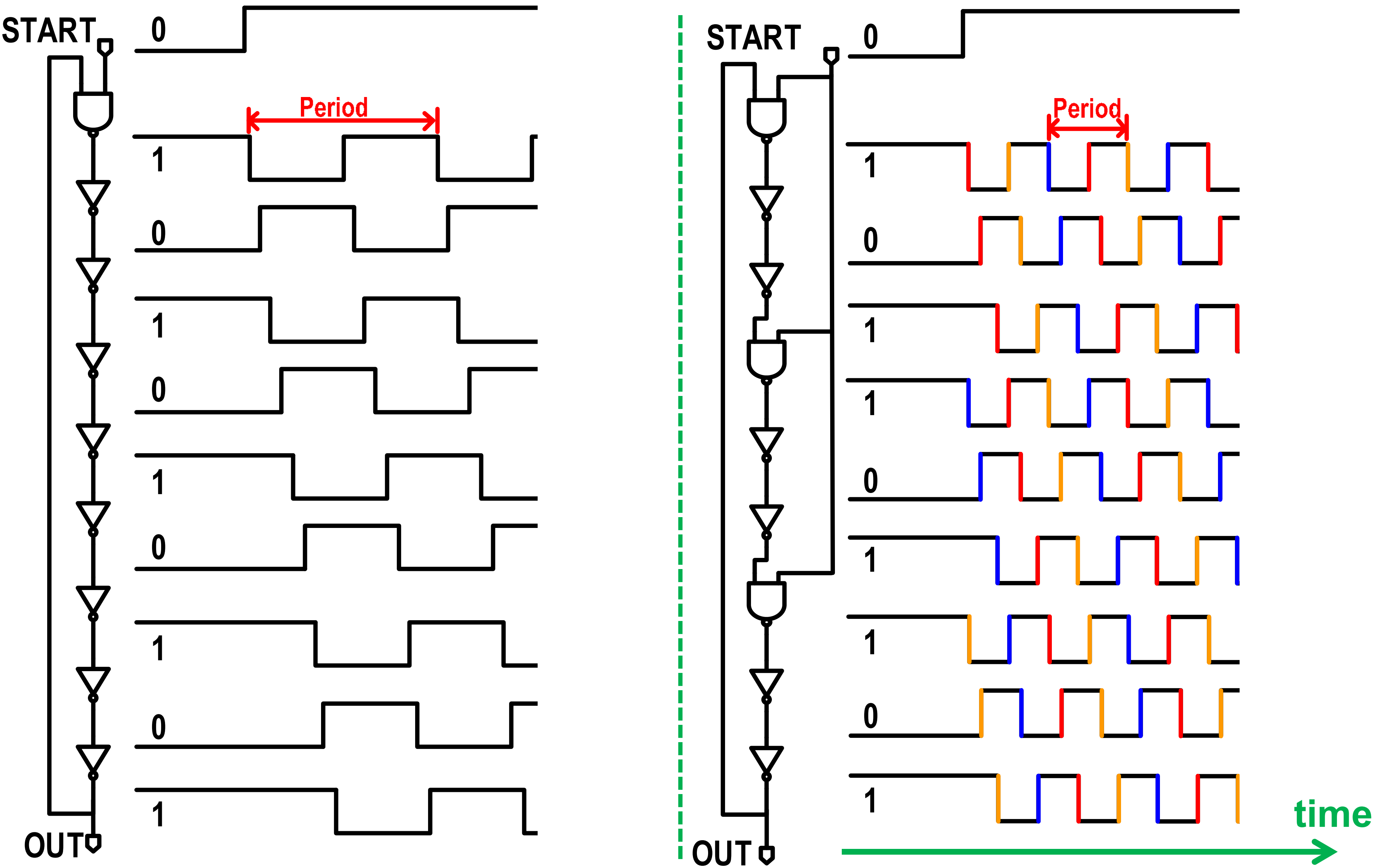
Multi-Mode Oscillator



Multi-Mode Oscillator

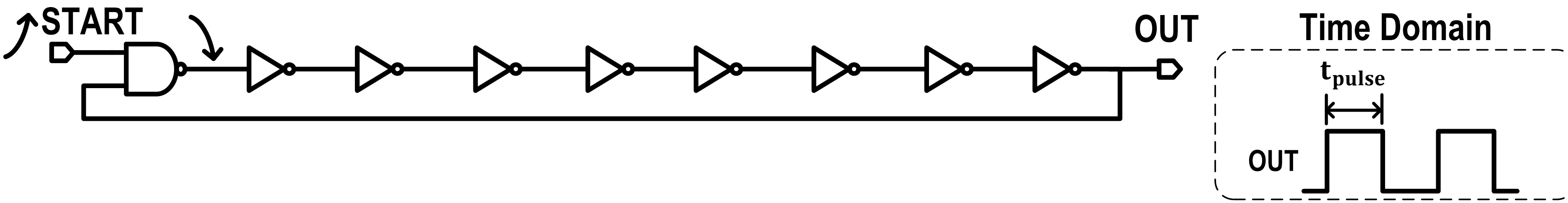


Multi-Mode Oscillator

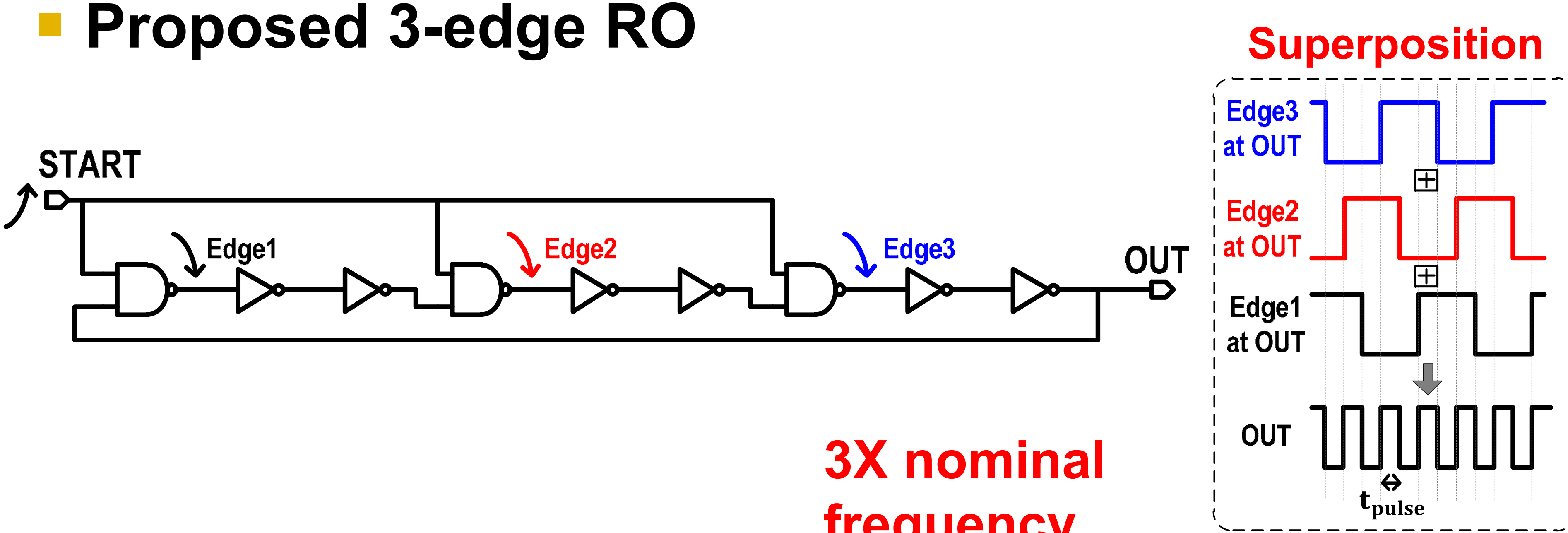


Multi-Mode Oscillator

- Ring oscillator (RO)

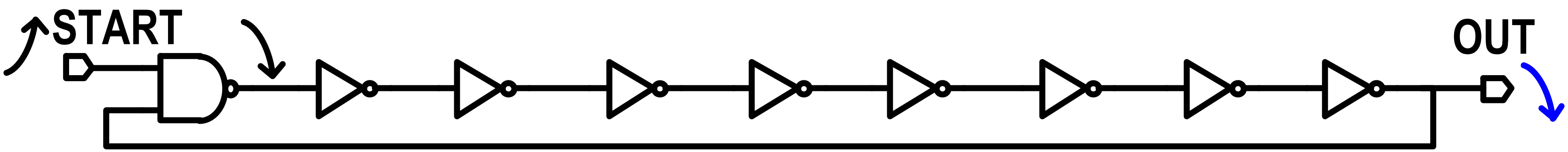


- Proposed 3-edge RO



3X nominal frequency

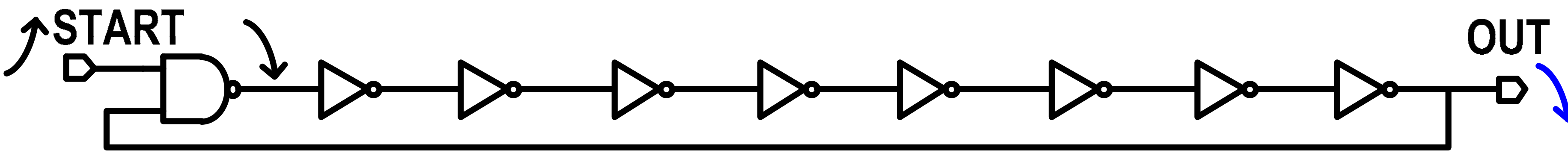
Jitter in 1-edge RO



Delay of i_{th} stage at c_{th} cycle: $T_i + \overline{\Delta t}_{c,i}\ , \overline{\Delta t}_{c,i} \sim N(0\ ,\ \sigma^2)$

systematic random

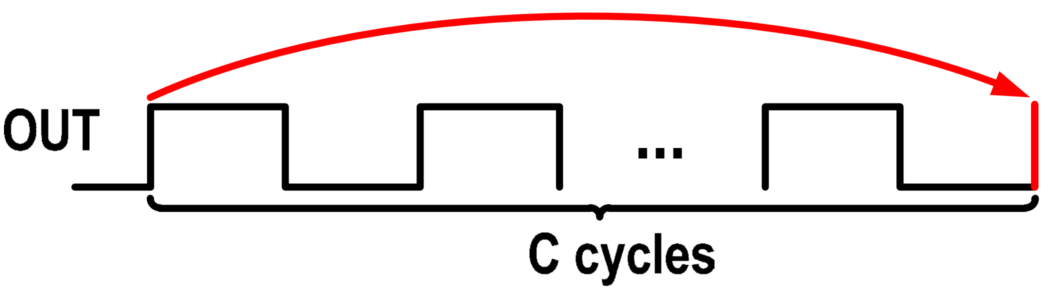
Jitter in 1-edge RO



Delay of i_{th} stage at c_{th} cycle: $T_i + \overline{\Delta t}_{c,i}$, $\overline{\Delta t}_{c,i} \sim N\left(0\,,\ \sigma^2\right)$

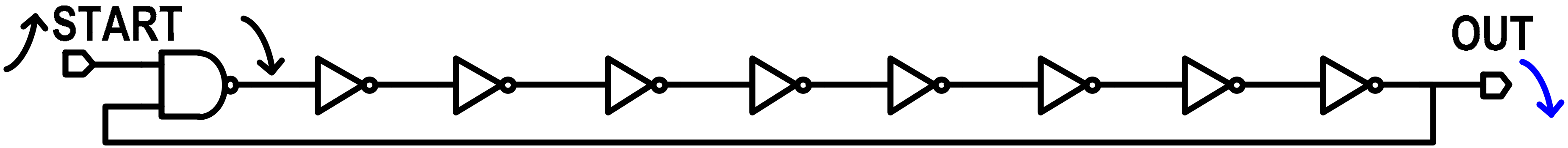
systematic random

S - # stages in RO
C - # cycles passed



$$T_{rise} = \sum_{c=1}^{C} \sum_{i=1}^{S} \left(T_i + \overline{\Delta t}_{c,i}\right)$$

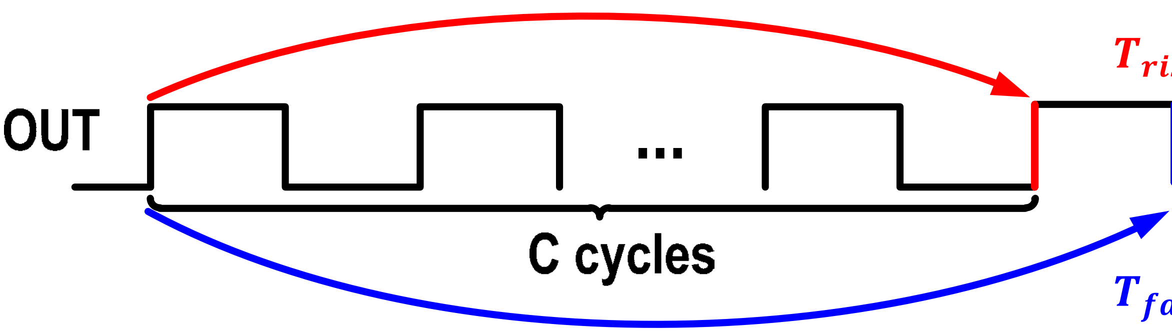
Jitter in 1-edge RO



Delay of i_{th} stage at c_{th} cycle: $T_i + \overline{\Delta t}_{c,i}$, $\overline{\Delta t}_{c,i} \sim N(0\,,\ \sigma^2)$

systematic random

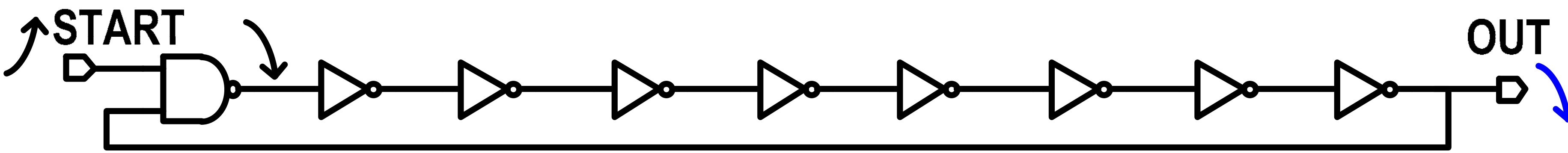
S - # stages in RO
C - # cycles passed



$$T_{rise} = \sum_{c=1}^{C} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{c,i})$$

$$T_{fall} = \sum_{c=1}^{C+1} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{c,i})$$

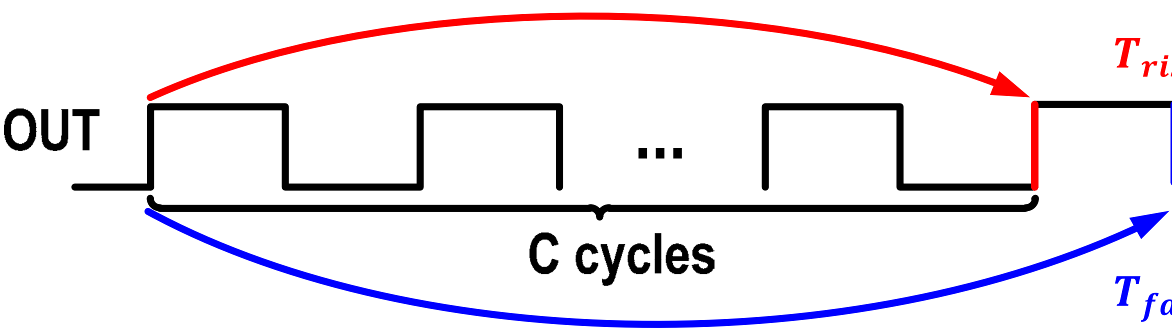
Jitter in 1-edge RO



Delay of i_{th} stage at c_{th} cycle: $T_i + \overline{\Delta t}_{c,i}\ ,\ \overline{\Delta t}_{c,i} \sim N(0\ ,\ \sigma^2)$

systematic random

S - # stages in RO
C - # cycles passed

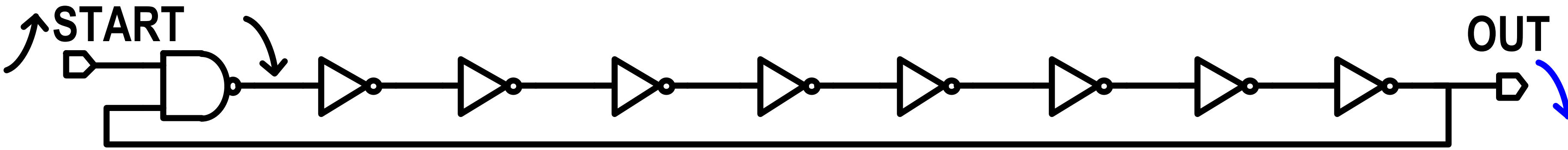


$$T_{rise} = \sum_{c=1}^{C} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{c,i})$$

$$T_{fall} = \sum_{c=1}^{C+1} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{c,i})$$

$$T_{pulse} = T_{fall} - T_{rise} = \sum_{c=C}^{C+1} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{n,i}) = \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{K,i}) \sim N(S \cdot T_i\ , S \cdot \sigma^2)$$

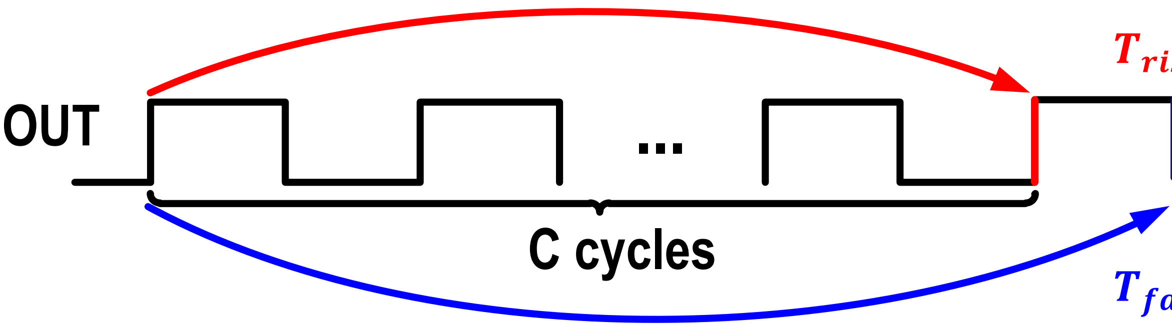
Jitter in 1-edge RO



Delay of i_{th} stage at c_{th} cycle: $T_i + \overline{\Delta t}_{c,i}$, $\overline{\Delta t}_{c,i} \sim N(0\,,\ \sigma^2)$

systematic random

S - # stages in RO
C - # cycles passed



$$T_{rise} = \sum_{c=1}^{C} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{c,i})$$

$$T_{fall} = \sum_{c=1}^{C+1} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{c,i})$$

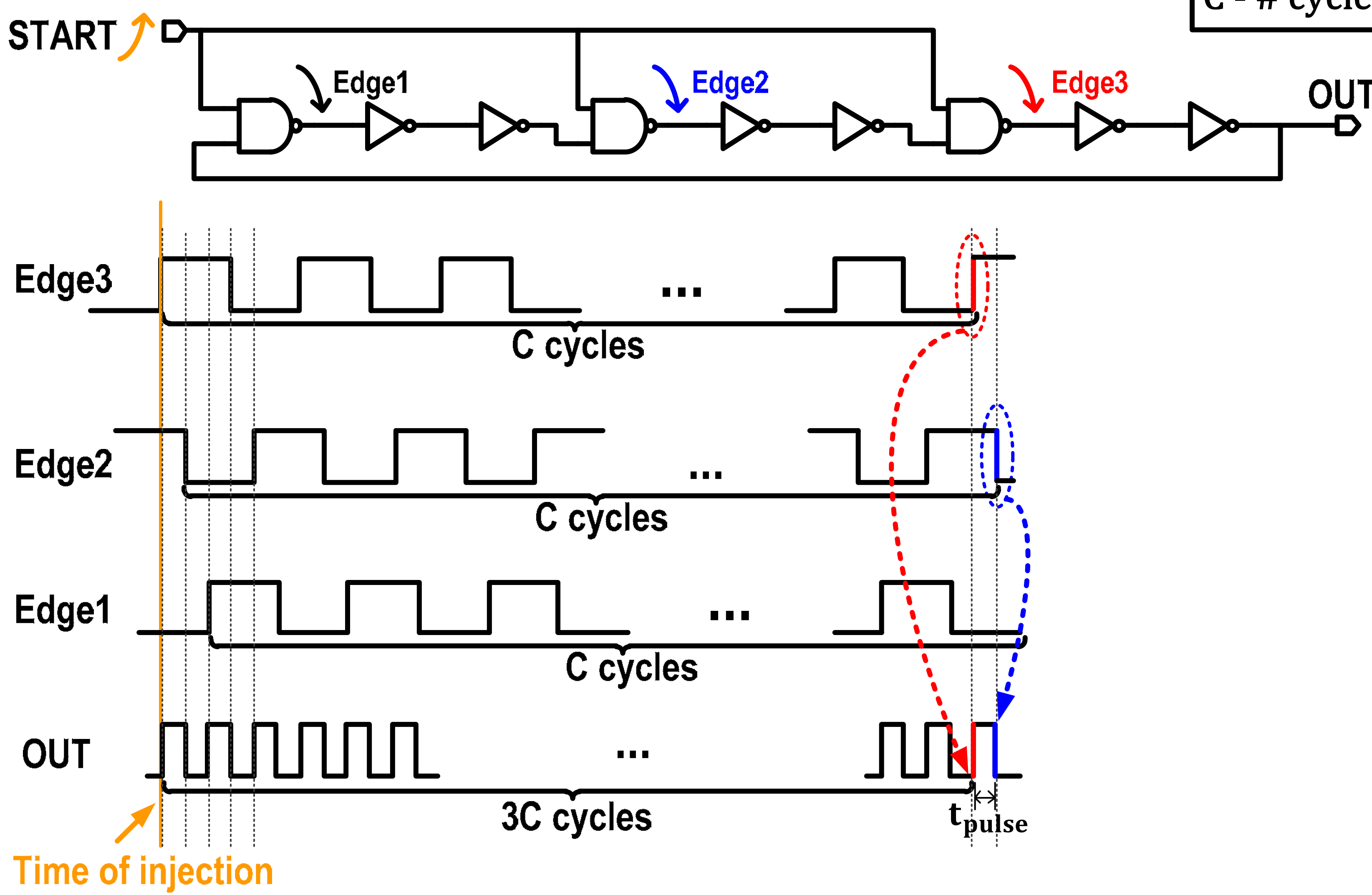
$$T_{pulse} = T_{fall} - T_{rise} = \sum_{c=C}^{C+1} \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{n,i}) = \sum_{i=1}^{S} (T_i + \overline{\Delta t}_{K,i}) \sim N(S \cdot T_i\,, S \cdot \sigma^2)$$

Not a function of cycle count!

Collapse in Proposed 3-edge RO

- **Waveform seen at output node of 3rd NAND**

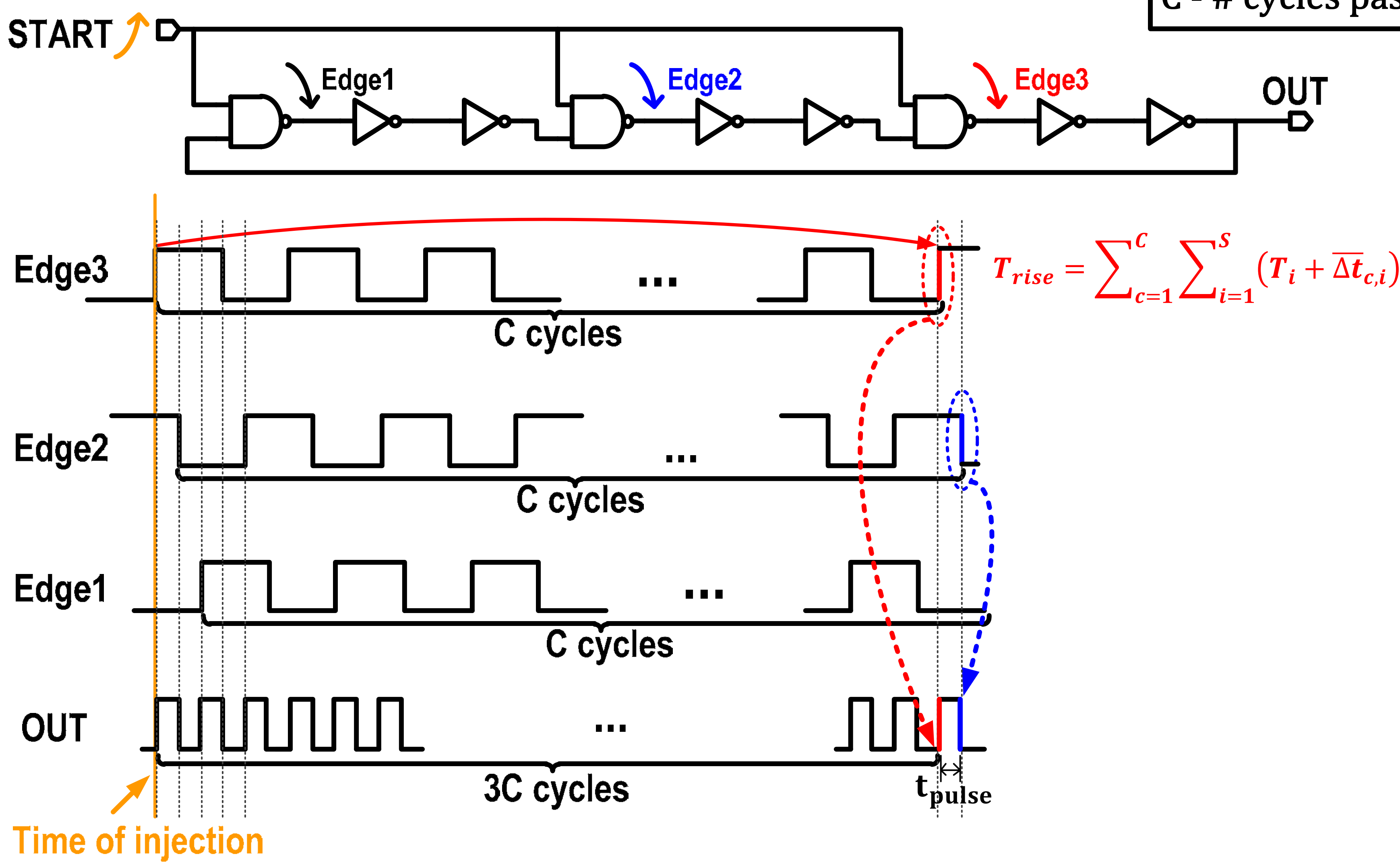
S - # stages in RO
C - # cycles passed



Collapse in Proposed 3-edge RO

- **Waveform seen at output node of 3rd NAND**

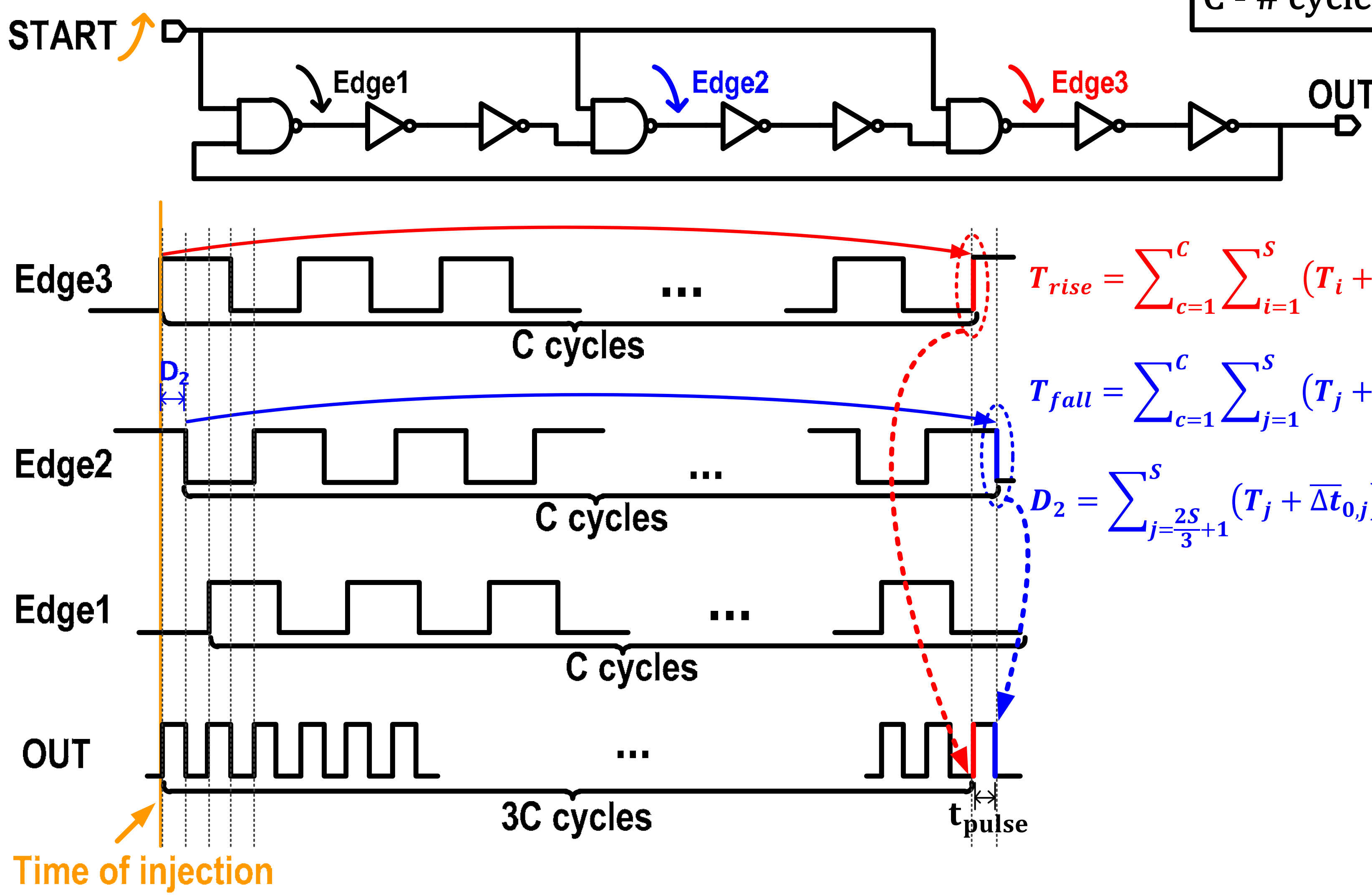
S - # stages in RO
C - # cycles passed



Collapse in Proposed 3-edge RO

- **Waveform seen at output node of 3rd NAND**

S - # stages in RO
C - # cycles passed



$$T_{rise} = \sum_{c=1}^{C}\sum_{i=1}^{S}\left(T_i + \overline{\Delta t}_{c,i}\right)$$

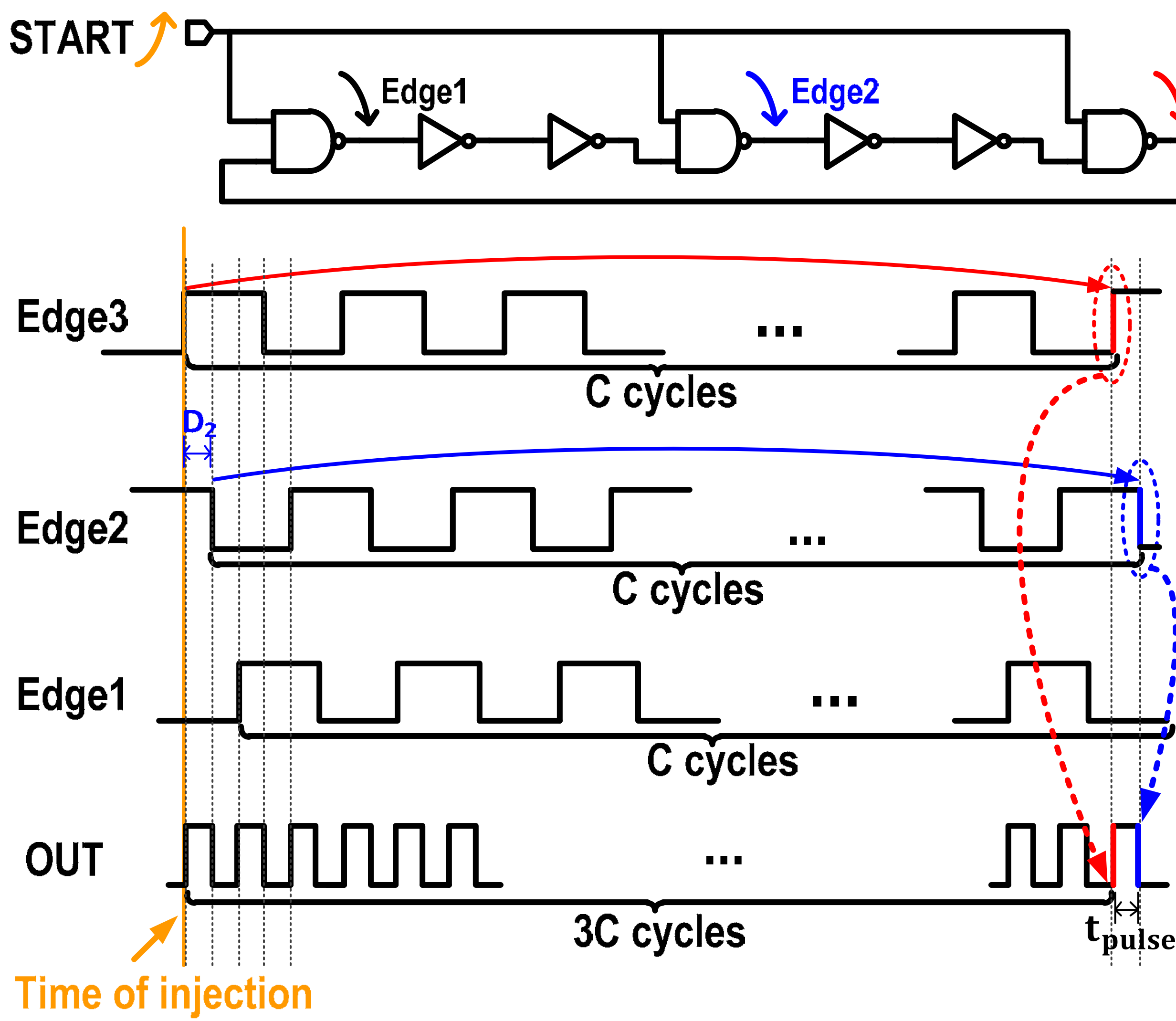
$$T_{fall} = \sum_{c=1}^{C}\sum_{j=1}^{S}\left(T_j + \overline{\Delta t}_{c,j}\right) + D_2$$

$$D_2 = \sum_{j=\frac{2S}{3}+1}^{S}\left(T_j + \overline{\Delta t}_{0,j}\right)$$

Collapse in Proposed 3-edge RO

- **Waveform seen at output node of 3rd NAND**

S - # stages in RO
C - # cycles passed



$$T_{rise} = \sum_{c=1}^{C}\sum_{i=1}^{S}\left(T_i + \overline{\Delta t}_{c,i}\right)$$

$$T_{fall} = \sum_{c=1}^{C}\sum_{j=1}^{S}\left(T_j + \overline{\Delta t}_{c,j}\right) + D_2$$

$$D_2 = \sum_{j=\frac{2S}{3}+1}^{S}\left(T_j + \overline{\Delta t}_{0,j}\right)$$

independent

$$T_{pulse} = T_{fall} - T_{rise}$$

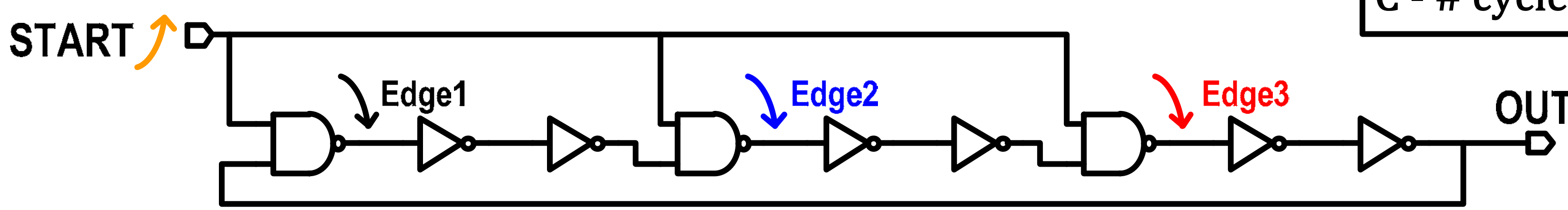
$$= \sum_{c=1}^{C}\sum_{i,j=1}^{S}\left(\boxed{\Delta t_{c,j}} - \boxed{\Delta t_{c,i}}\right) + D_2$$

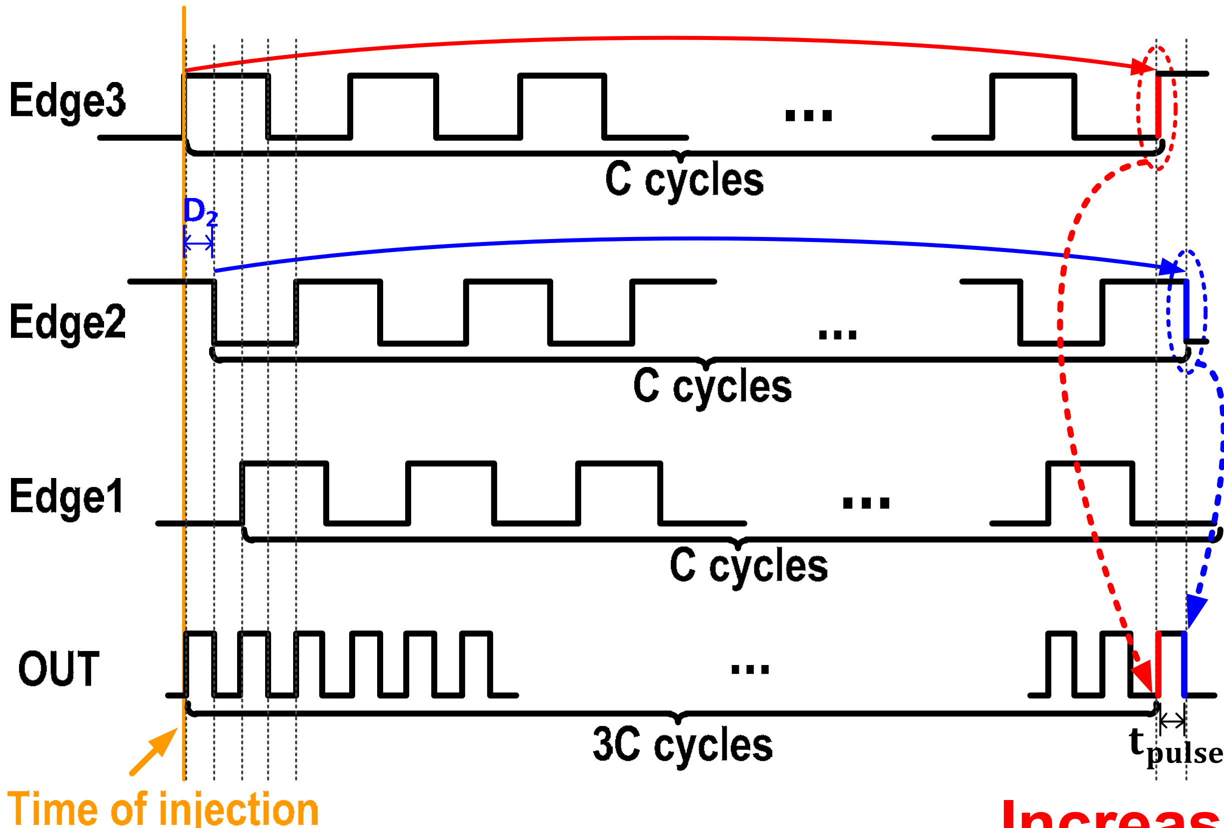
$$\sim N\left(D_2\,, C \cdot S \cdot \sigma^2\right)$$

Collapse in Proposed 3-edge RO

- **Waveform seen at output node of 3rd NAND**

S - # stages in RO
C - # cycles passed





$$T_{rise} = \sum_{c=1}^{C}\sum_{i=1}^{S}\left(T_i + \overline{\Delta t}_{c,i}\right)$$

$$T_{fall} = \sum_{c=1}^{C}\sum_{j=1}^{S}\left(T_j + \overline{\Delta t}_{c,j}\right) + D_2$$

$$D_2 = \sum_{j=\frac{2S}{3}+1}^{S}\left(T_j + \overline{\Delta t}_{0,j}\right)$$

independent

$$T_{pulse} = T_{fall} - T_{rise}$$

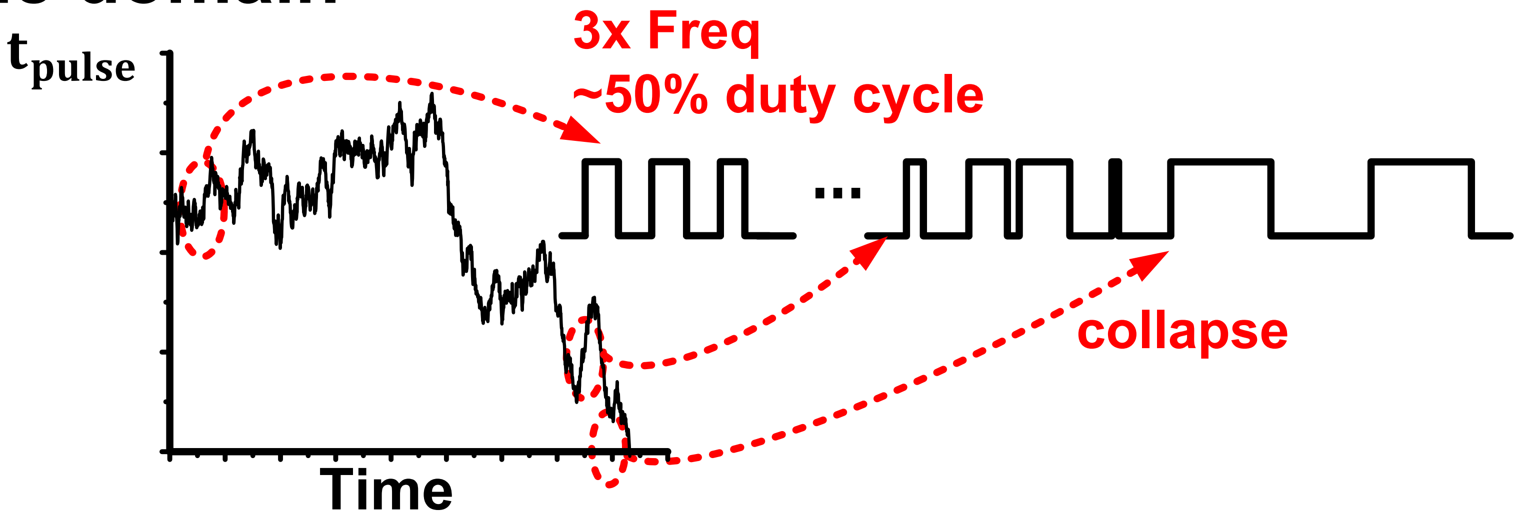
$$= \sum_{c=1}^{C}\sum_{i,j=1}^{S}\left(\boxed{\overline{\Delta t}_{c,j}} - \boxed{\overline{\Delta t}_{c,i}}\right) + D_2$$

$$\sim N\left(D_2, \boxed{C \cdot S \cdot \sigma^2}\right)$$

Increasing with cycle count!

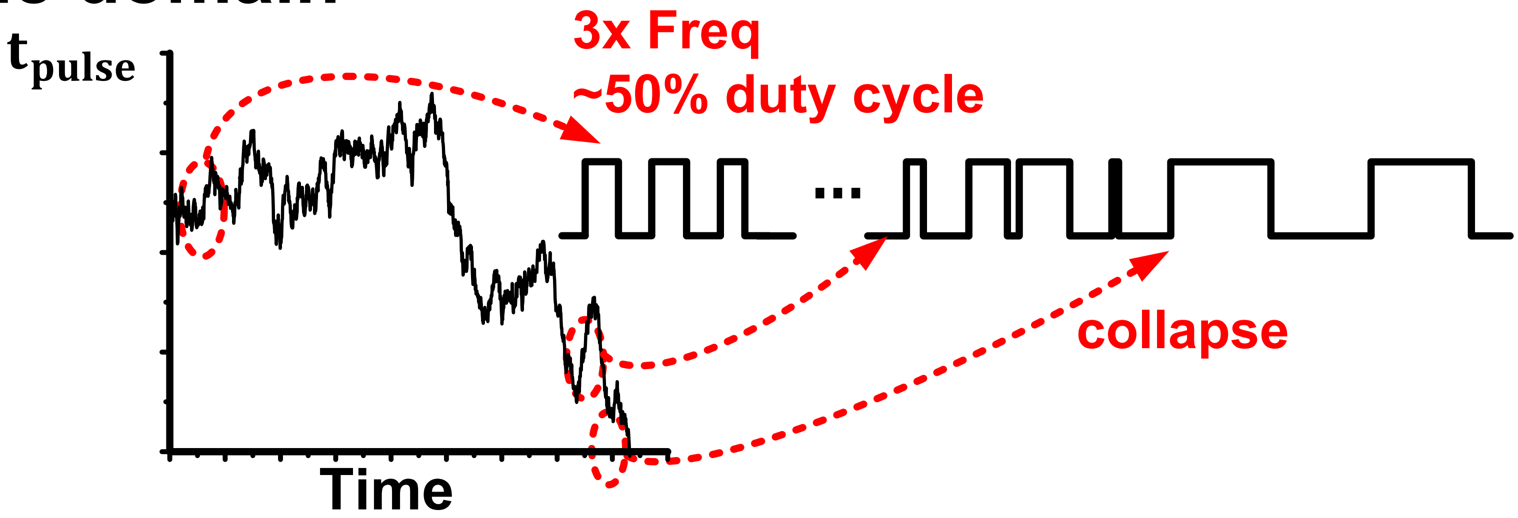
Collapse in Proposed 3-edge RO

- Time domain

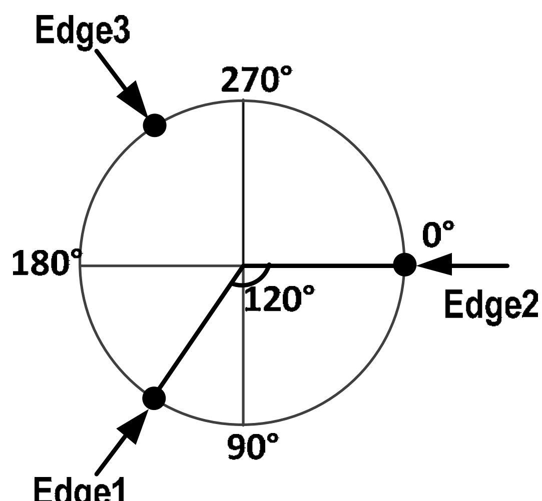


Collapse in Proposed 3-edge RO

- **Time domain**

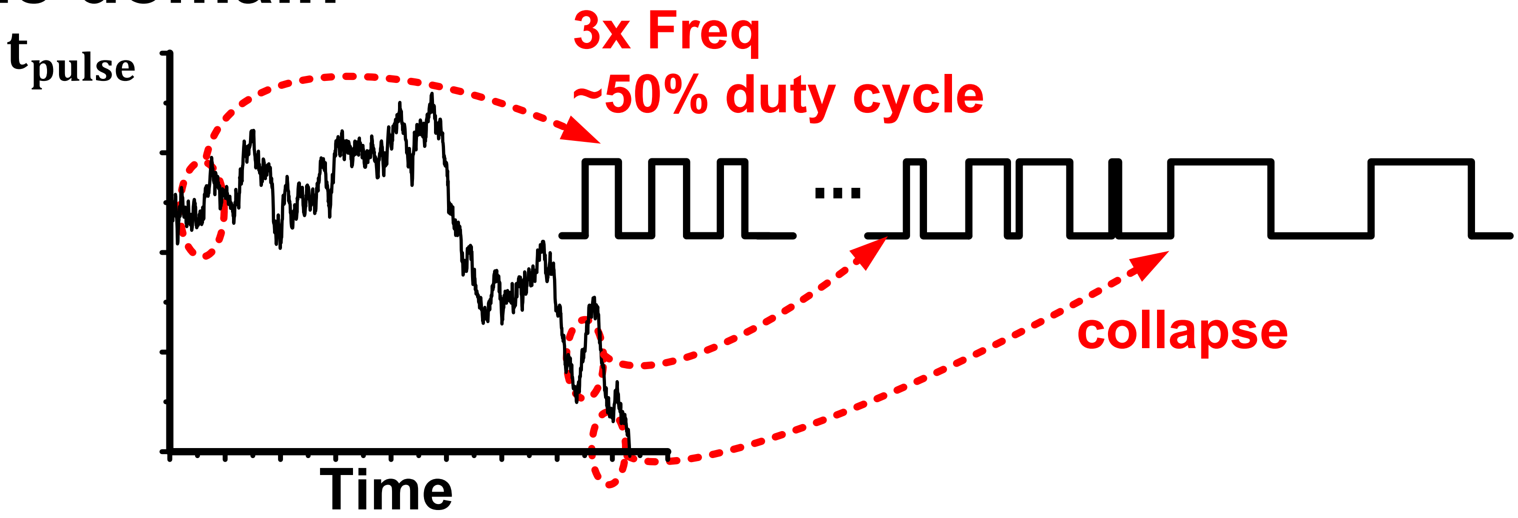


- **Phase domain**

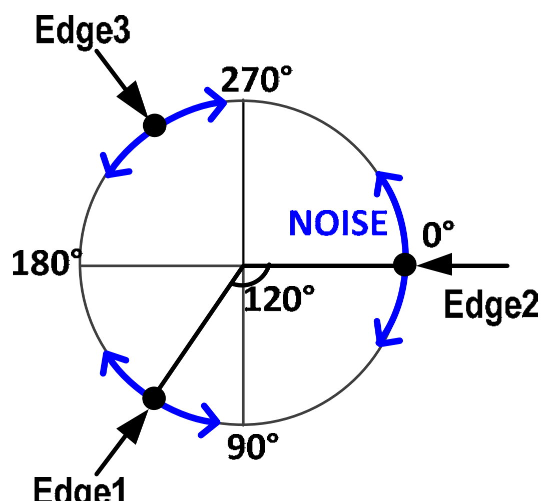


Collapse in Proposed 3-edge RO

- Time domain



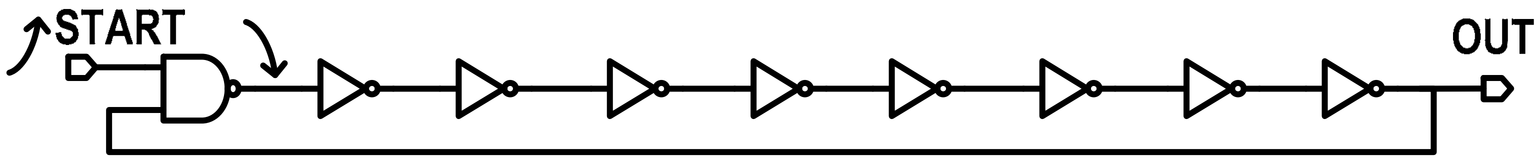
- Phase domain

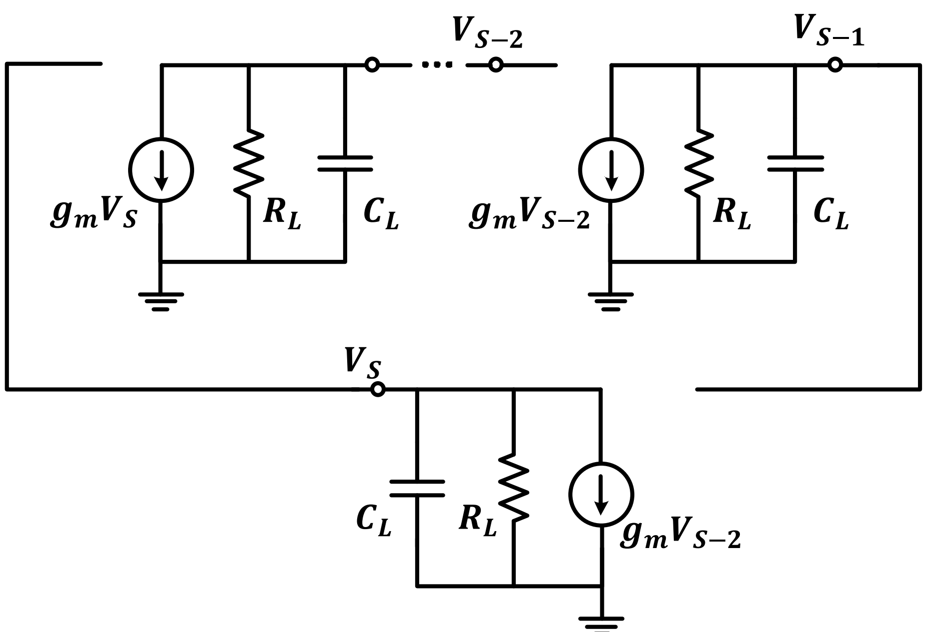


Multi-Mode Oscillator

- **Analysis from analog point of view**

S - # stages in RO





System zero

$$-\frac{1}{R_L C_L}$$

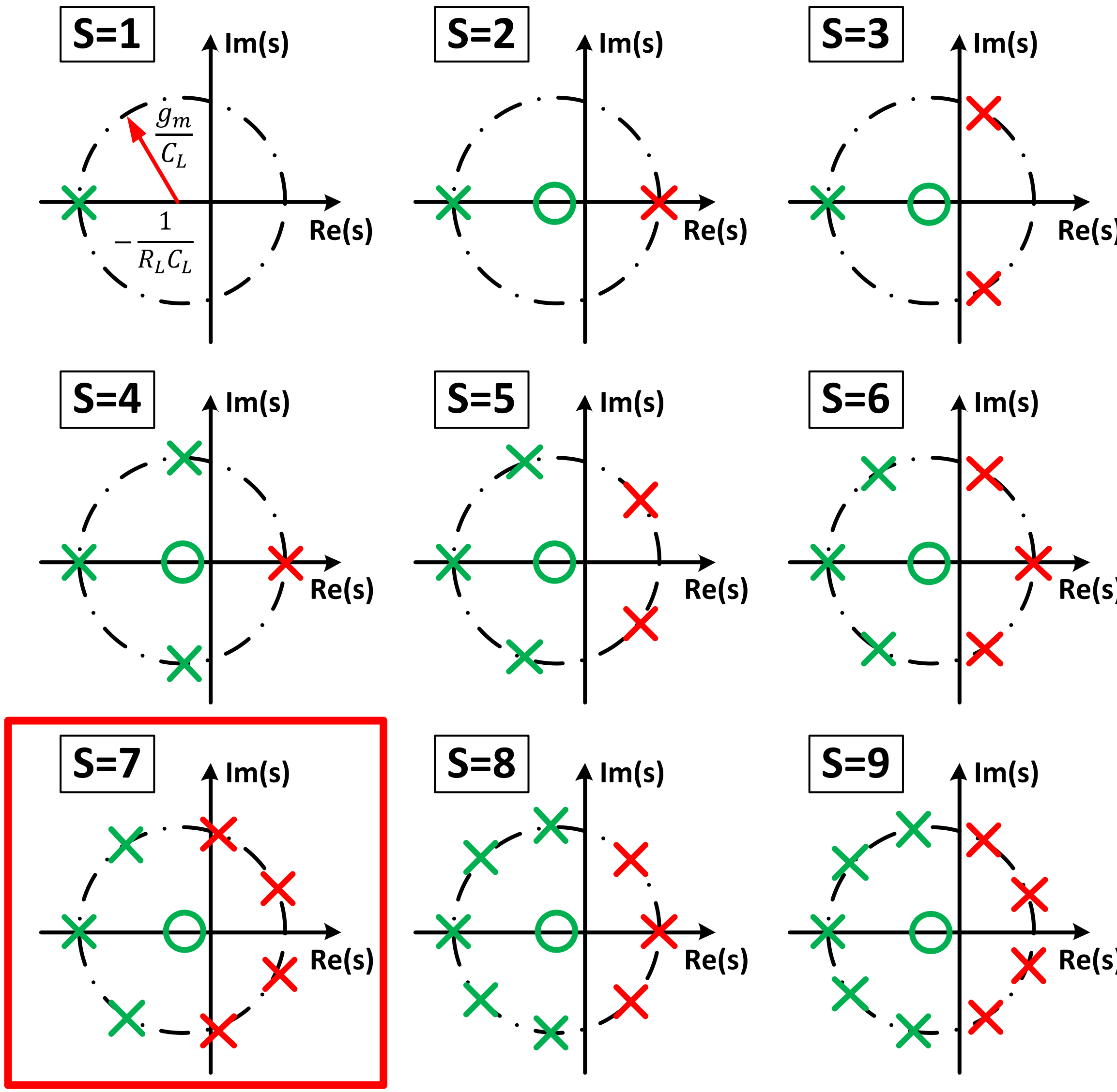
System poles

$$-\frac{g_m}{C_L} e^{\frac{j2n\pi}{S}} - \frac{1}{R_L C_L} \quad , n = 0, 1, 2, \ldots, S$$

Ref: J. de Cos, Trans. MTT, 2012

Multi-Mode Oscillator

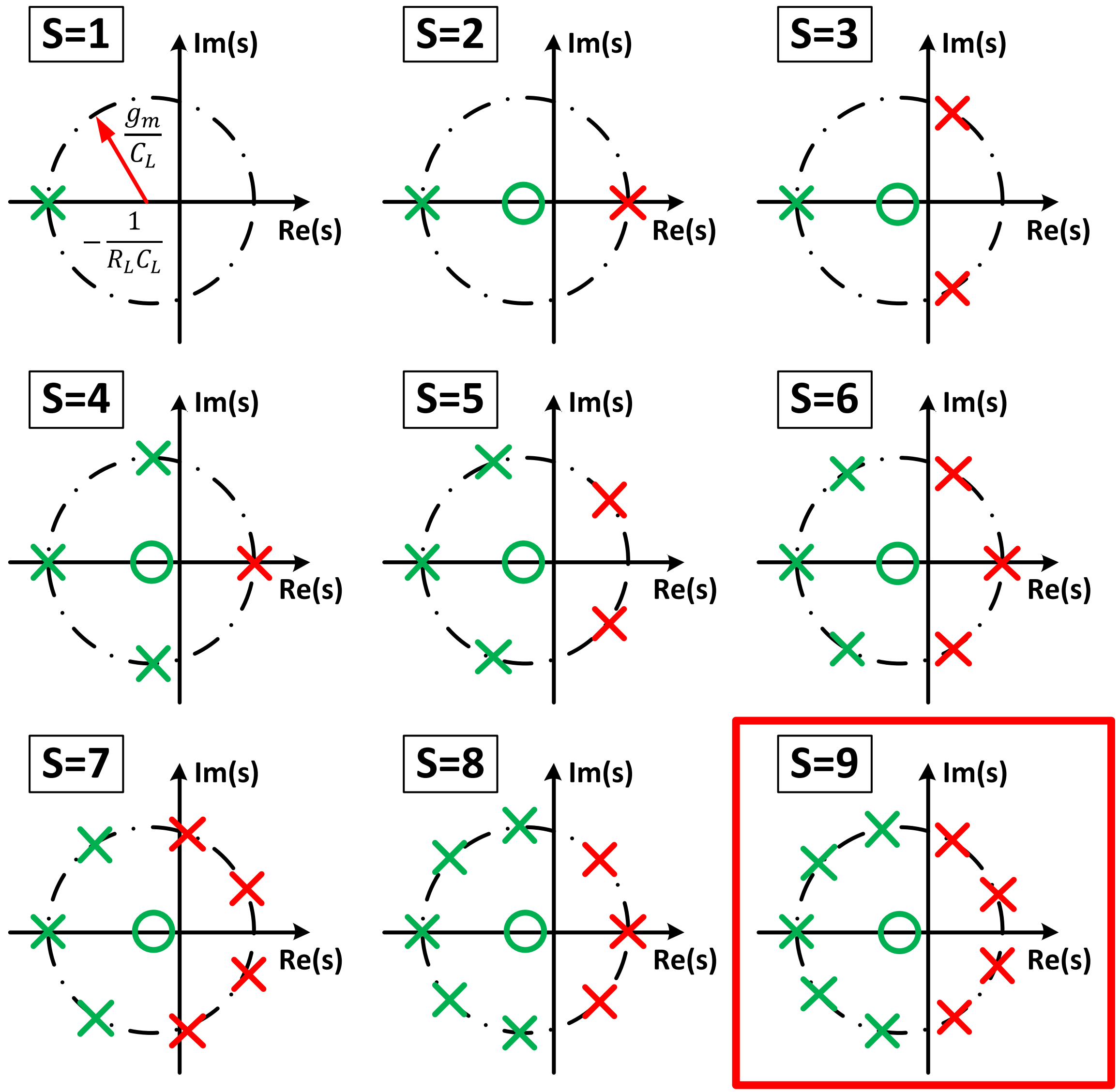
- **Pole/zero map**
  - When S≥7, it is possible to have 2+ oscillation modes



Ref: J. de Cos, Trans. MTT, 2012

Multi-Mode Oscillator

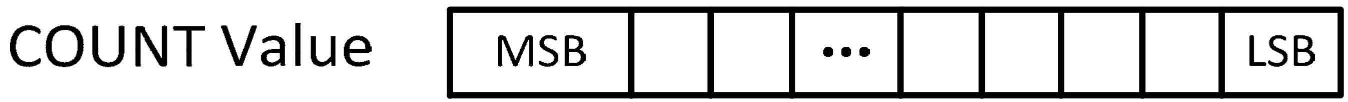
- **Pole/zero map**
  - When S≥7, it is possible to have 2+ oscillation modes
  - Our method of injection require number of stages to be multiples of 3

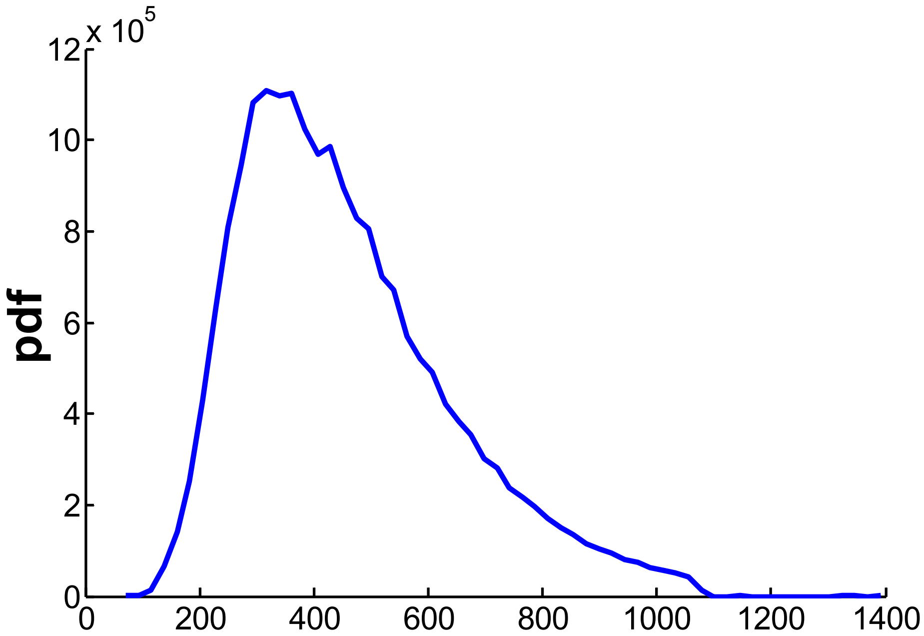


Ref: J. de Cos, Trans. MTT, 2012

Random bit generation

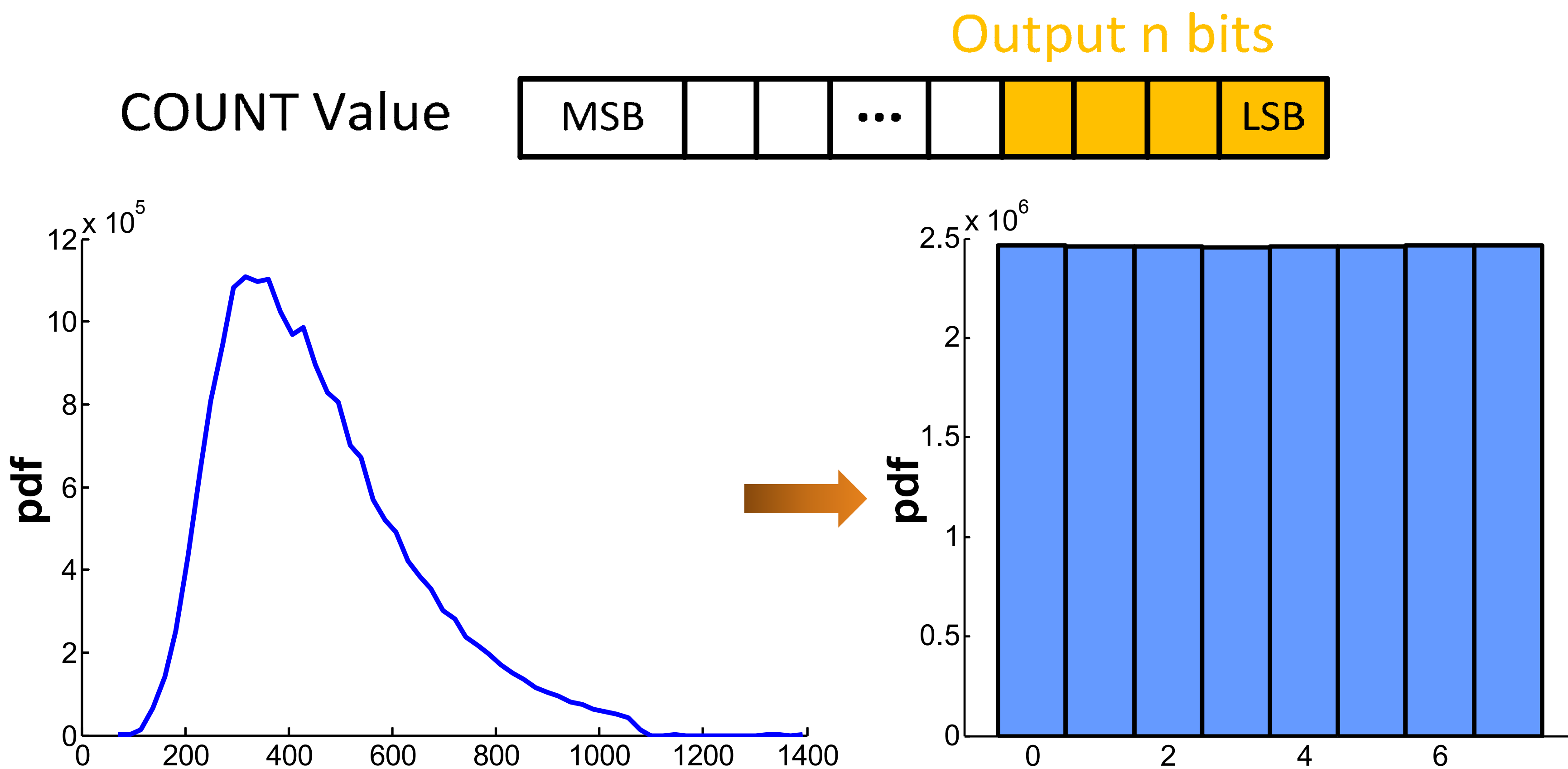
- **Time to collapse as entropy source**
  - Log-normal distribution





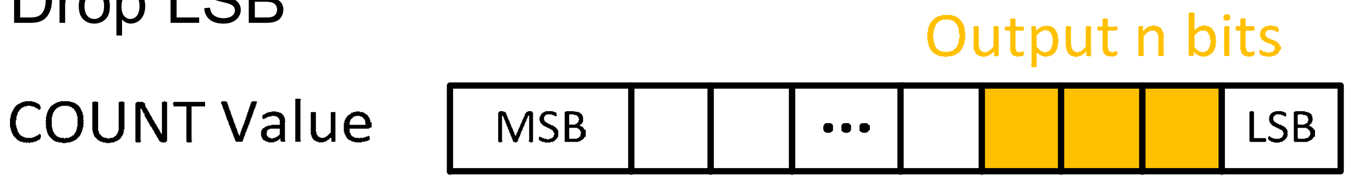
Random bit generation

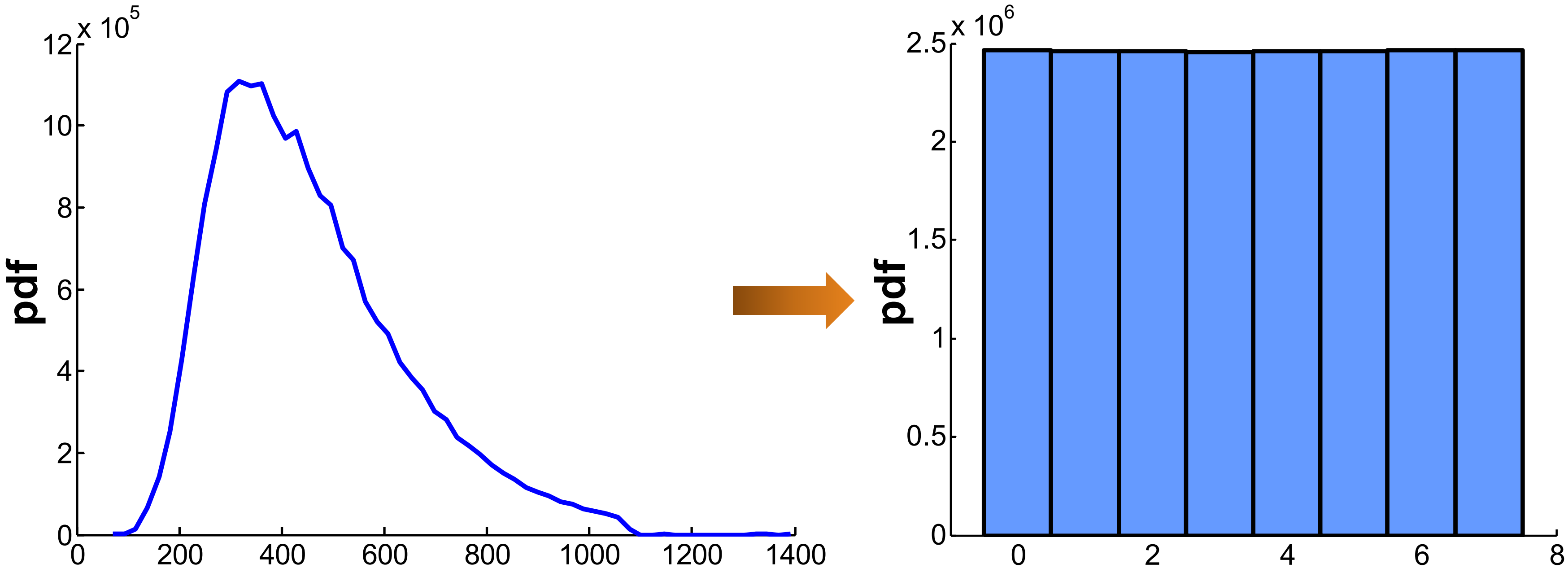
- **Time to collapse as entropy source**
  - Log-normal distribution
  - Truncate lower n bits as random bits



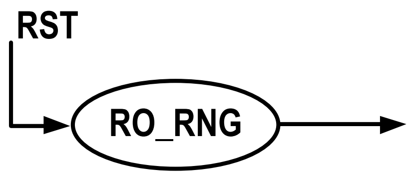
Random bit generation

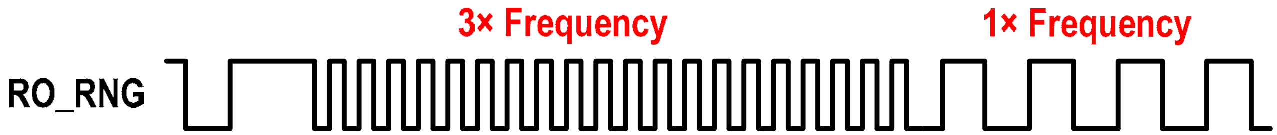
- **Time to collapse as entropy source**
  - Log-normal distribution
  - Truncate lower n bits as random bits
  - Drop LSB



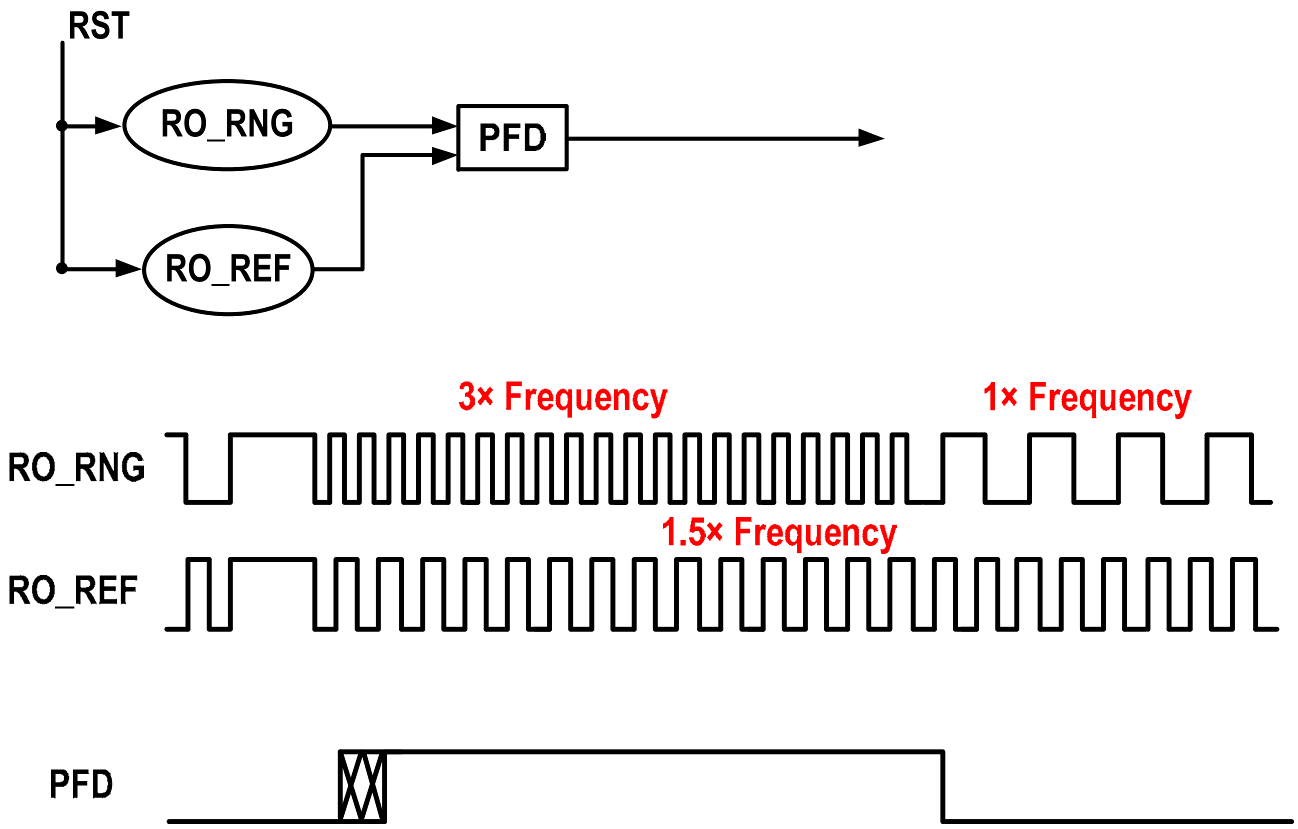


Proposed TRNG System

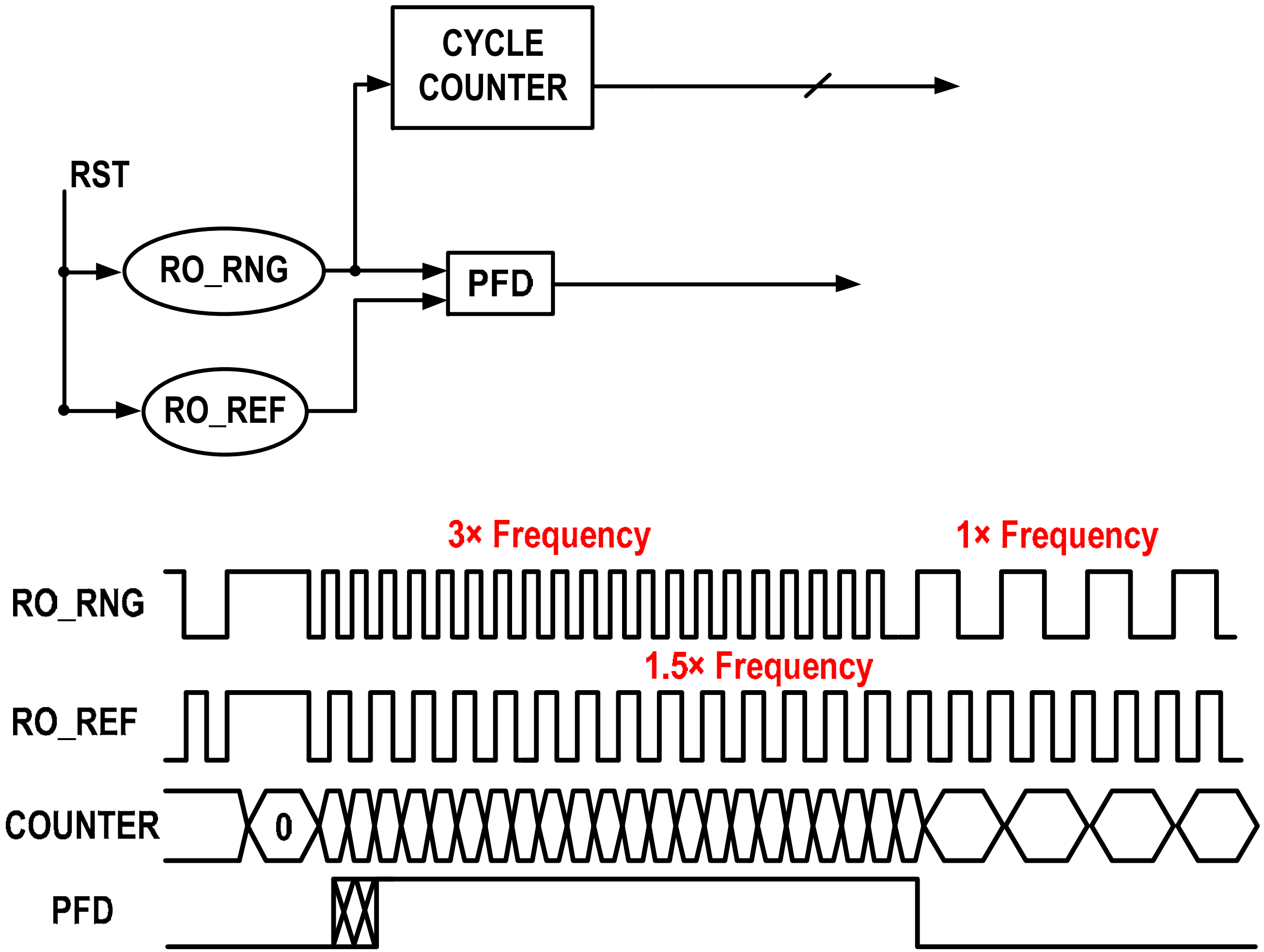




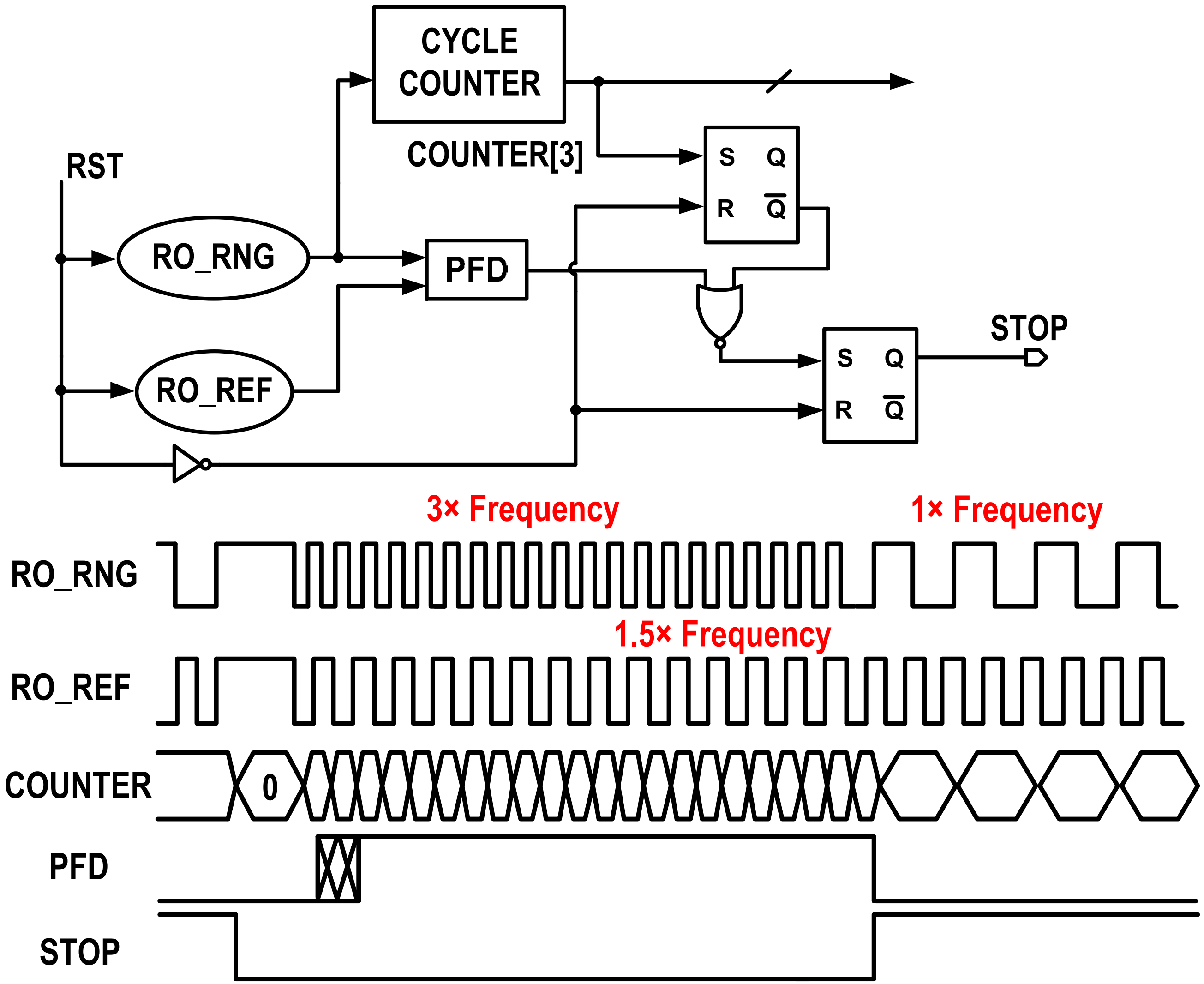
Proposed TRNG System



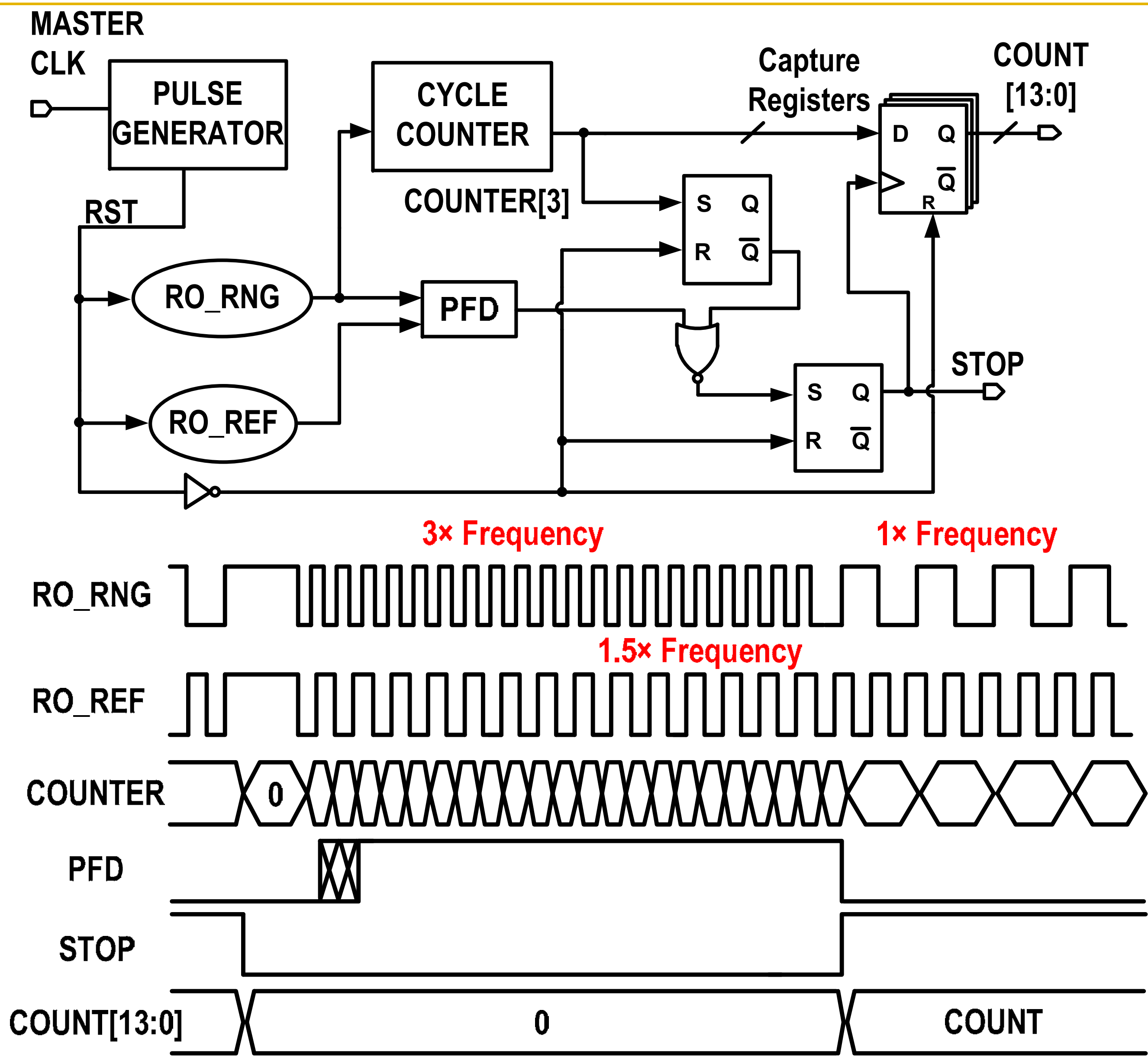
Proposed TRNG System



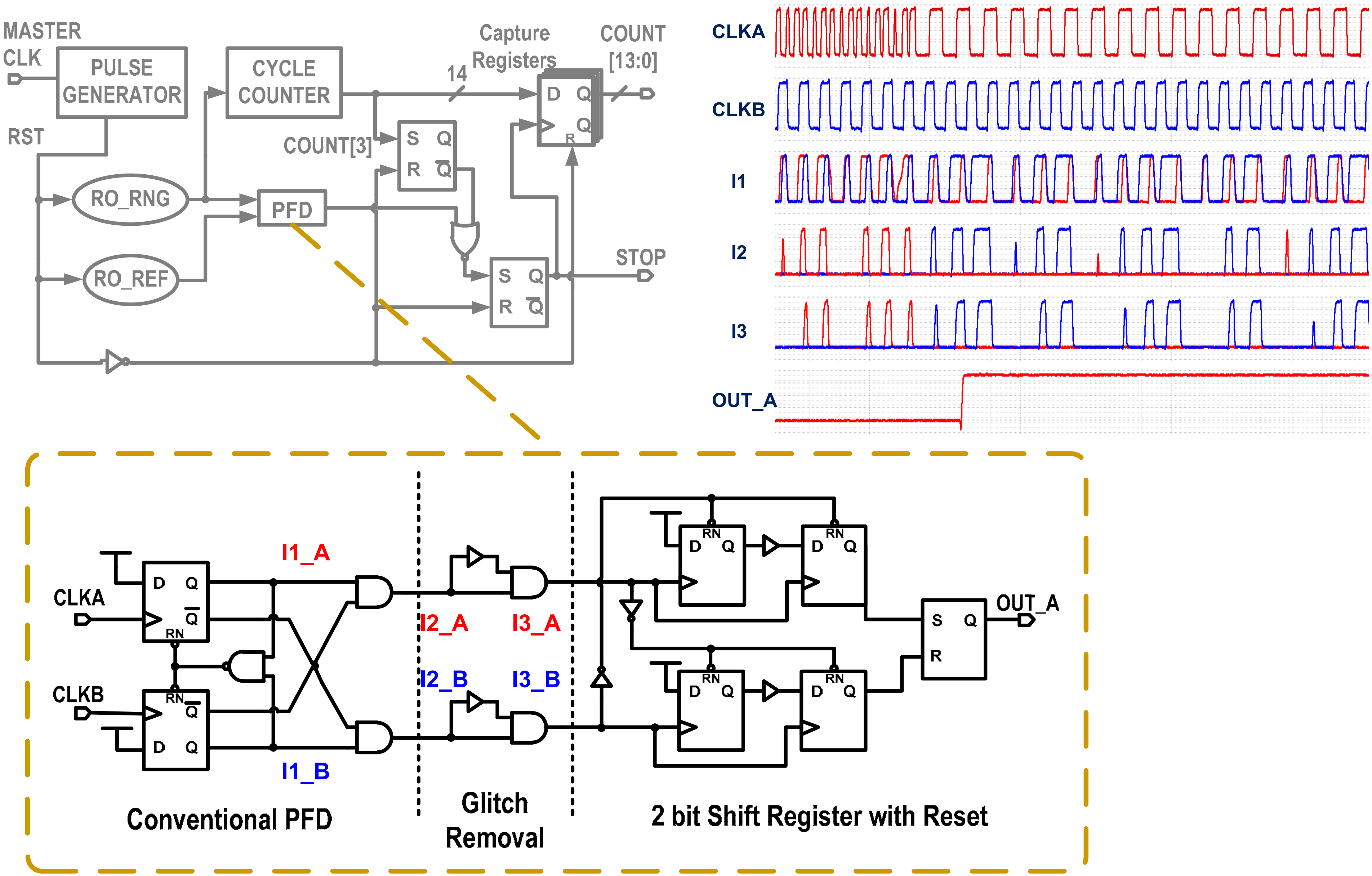
Proposed TRNG System



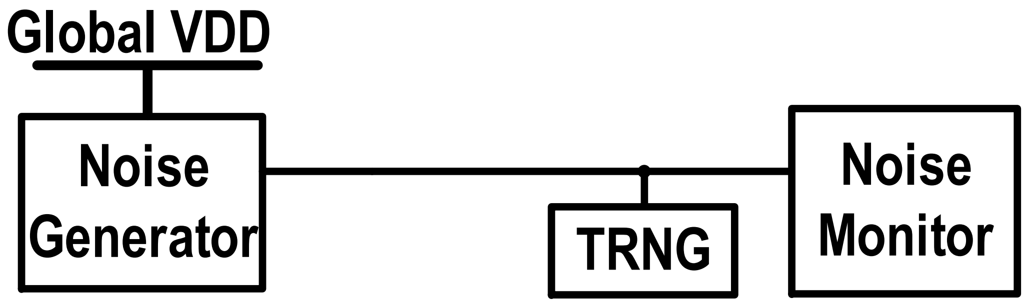
Proposed TRNG System



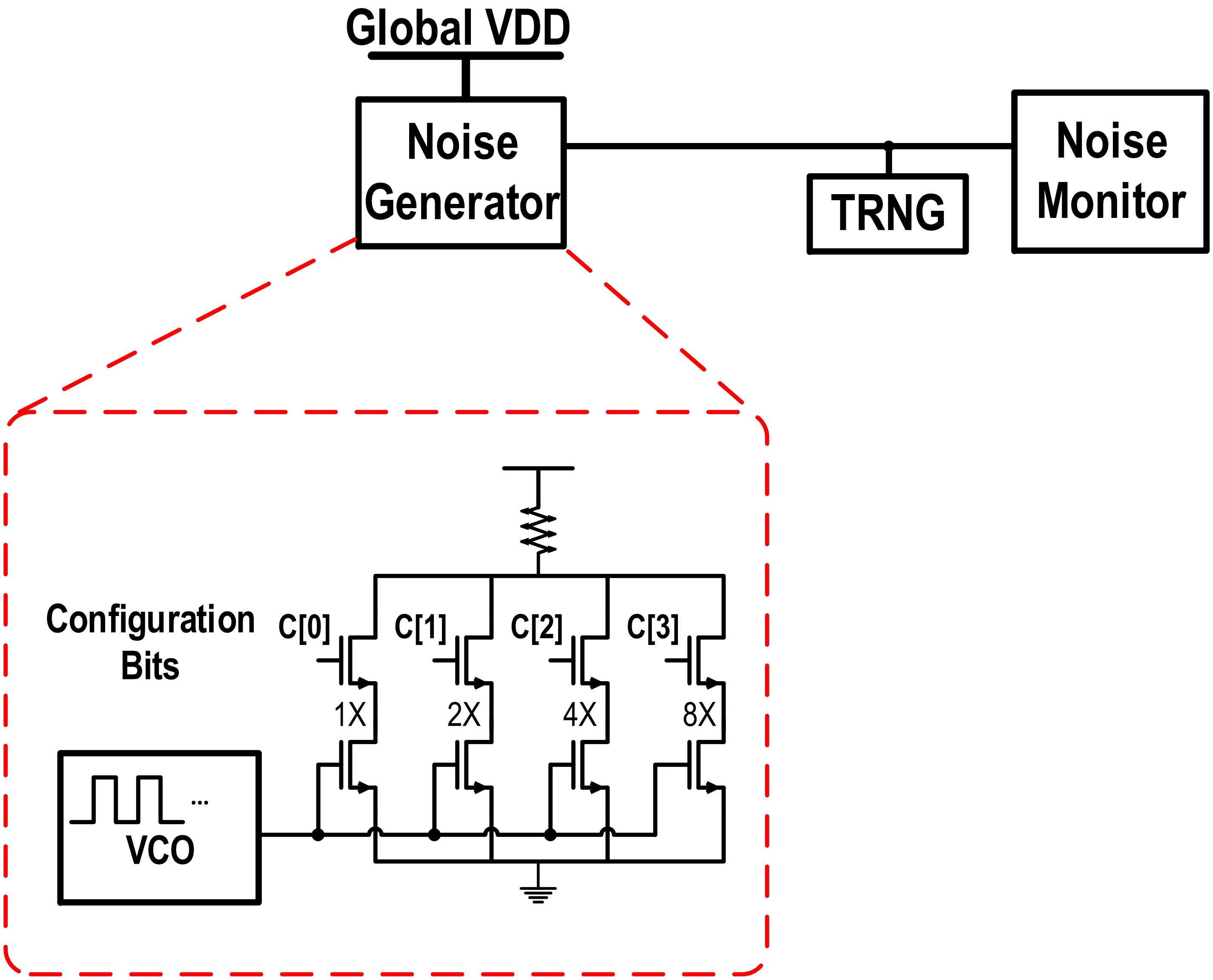
Phase Frequency Detector



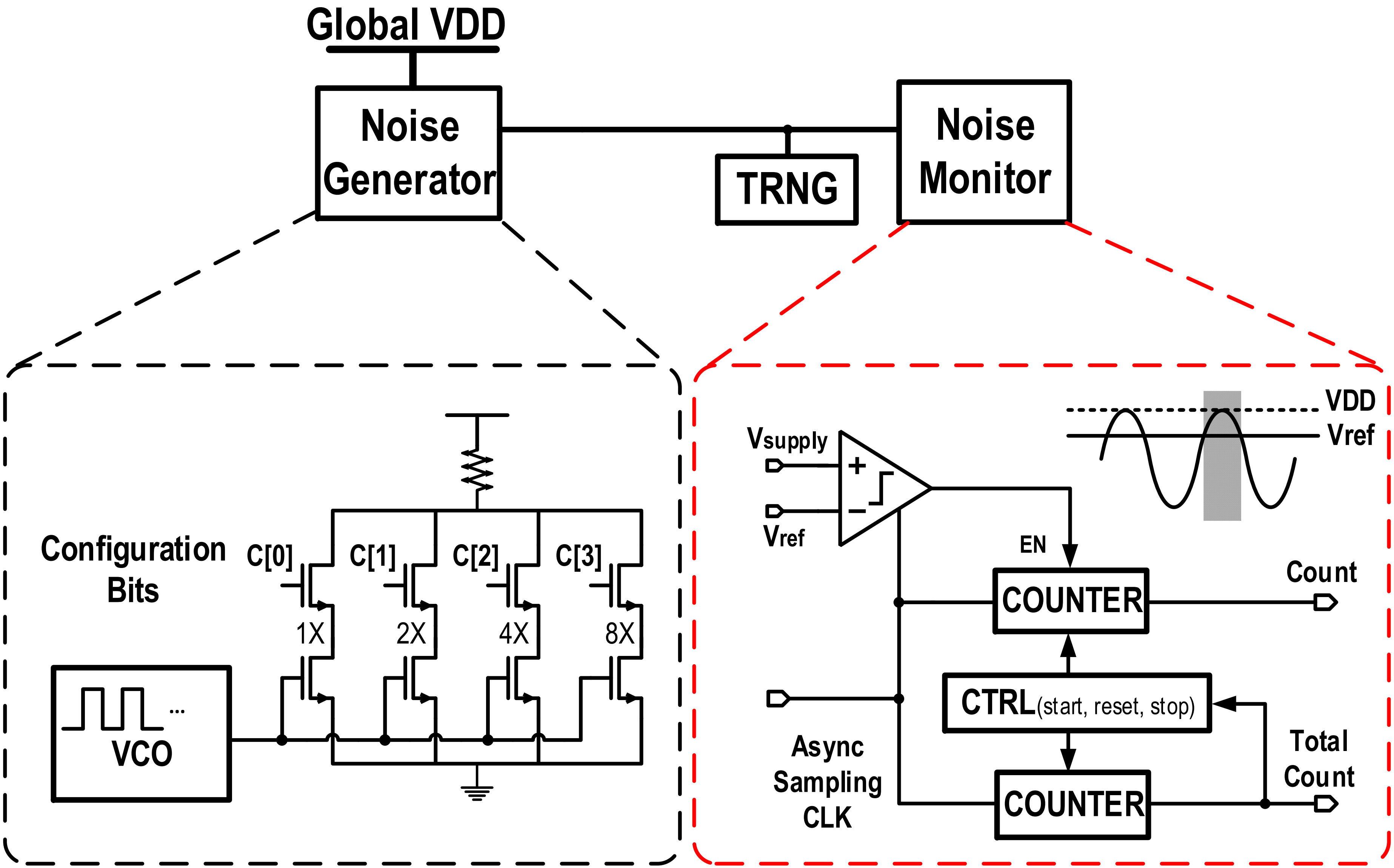
On-Chip Supply Noise Testing Setup



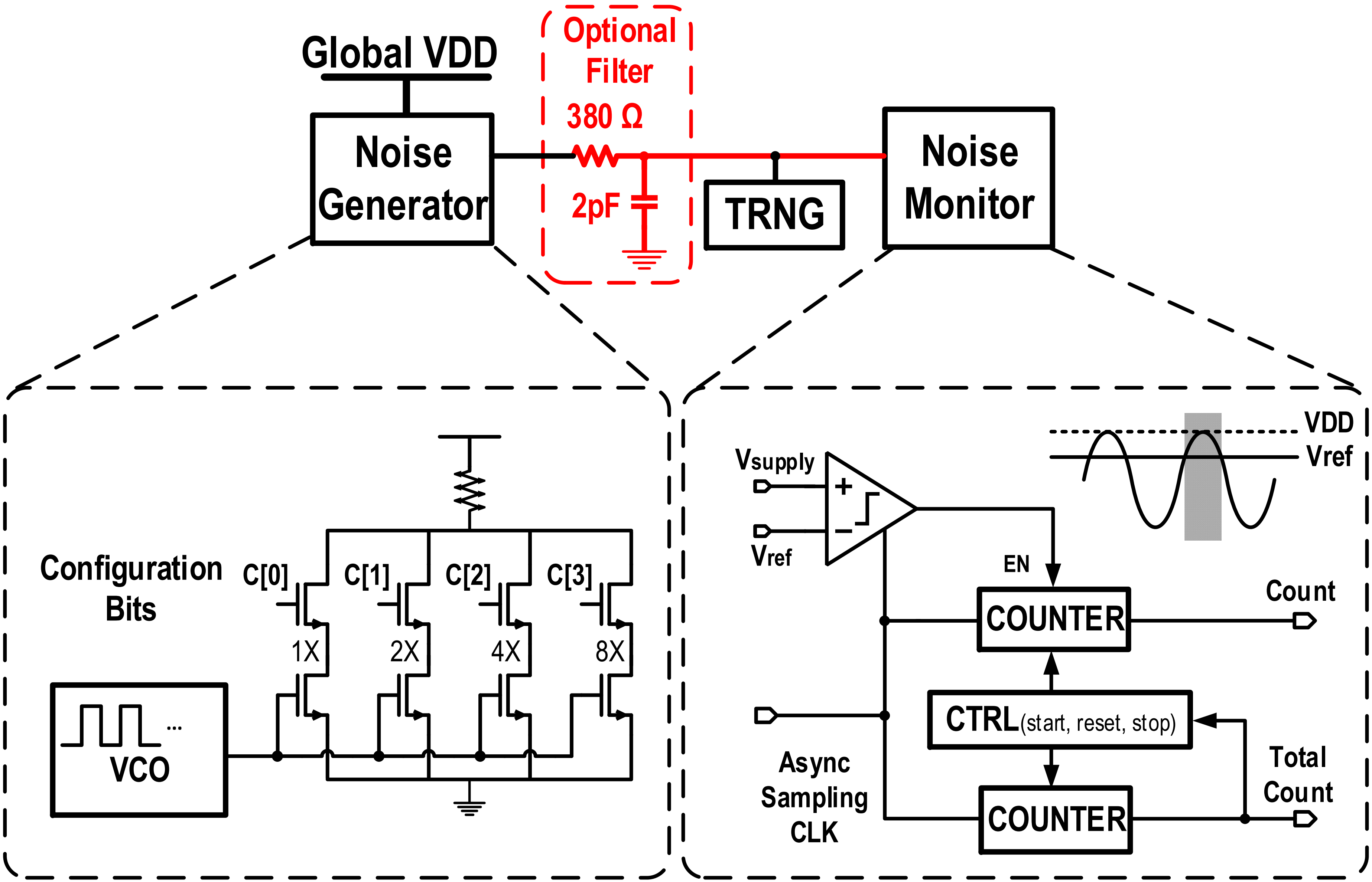
On-Chip Supply Noise Generator



On-Chip Supply Noise Monitor

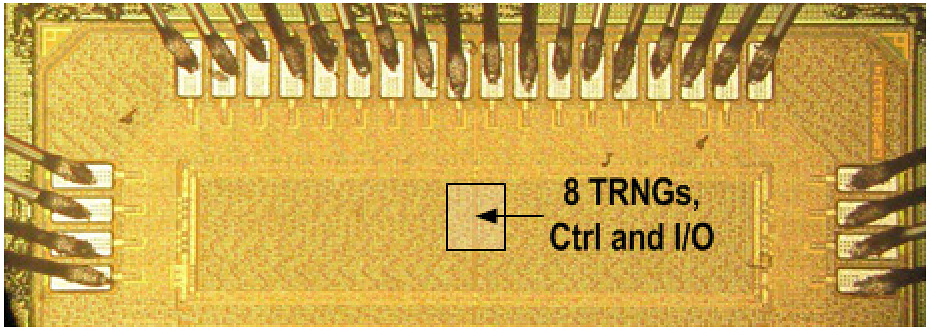


On-Chip Supply Noise Filter

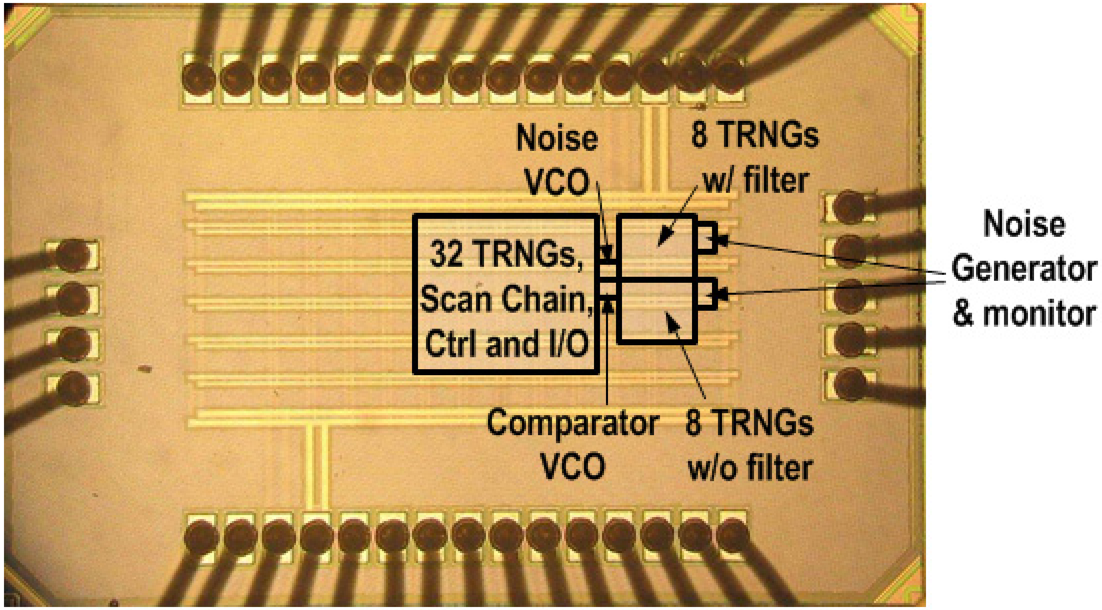


Test Chip

- **28nm prototype**
  - 8 TRNG variants
  - 375um^2 core area
  - 23.16 Mb/s
  - 23 pJ/bit
- **65nm prototype**
  - 32 TRNG variants
  - Supply noise testing setups
  - 960um^2 core area
  - 2.8 Mb/s
  - 57 pJ/bit



28nm Die Micrograph



65nm Die Micrograph

Randomness Test

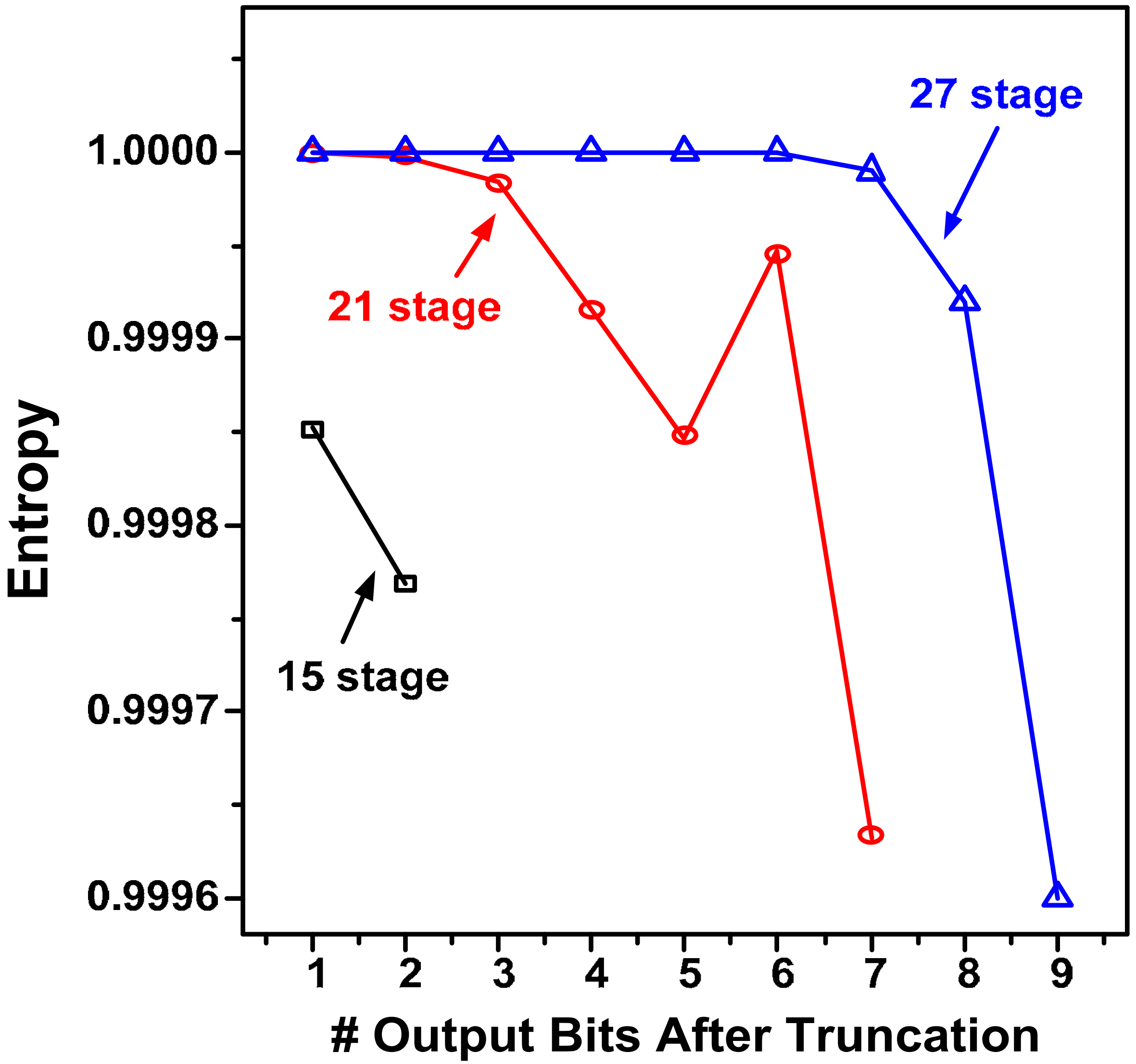
- **NIST Pub 800-22 testbench**
  - 100M bits collected
  - Min p-value is 0.01,
  - Min p-value χ^2 is 0.0001
  - Proposed TRNG consistently pass all NIST tests without post processing

NIST Pub 800-22, rev. 1a, 2010 Randomness Tests	65nm, 21 stage RO, 0.9V, 2.80Mb/s		28nm, 21 stage RO, 0.9V, 23.16Mb/s	
	P-value χ^2	Pass Rate	P-value χ^2	Pass Rate
Frequency	0.785562	296/300	0.872947	297/300
Block Frequency	0.082177	297/300	0.746572	297/300
Cumulativ Sum	0.462245	294/300	0.955835	296/300
Cumulativ Sum	0.942895	295/300	0.329332	294/300
Runs	0.220931	296/300	0.574903	297/300
Longest Runs	0.329332	296/300	0.81047	298/300
Matrix Rank	0.046668	294/300	0.000682	296/300
FFT	0.03013	295/300	0.224821	295/300
Non Overlapping Template	PASS*	PASS*	PASS*	PASS*
Overlapping Template	0.878107	297/300	0.329332	296/300
Linear Complexity	0.487885	297/300	0.304126	295/300
Universal	0.935716	98/100	0.719747	99/100
Random Excursions	PASS*	PASS*	PASS*	PASS*
Random Excursions Variant	PASS*	PASS*	PASS*	PASS*
Approximate Entropy	0.514124	100/100	0.275709	100/100
Serial	0.304126	99/100	0.897763	99/100
Serial	0.867692	99/100	0.595549	100/100

* "PASS" means all sub tests pass minimum requirement.

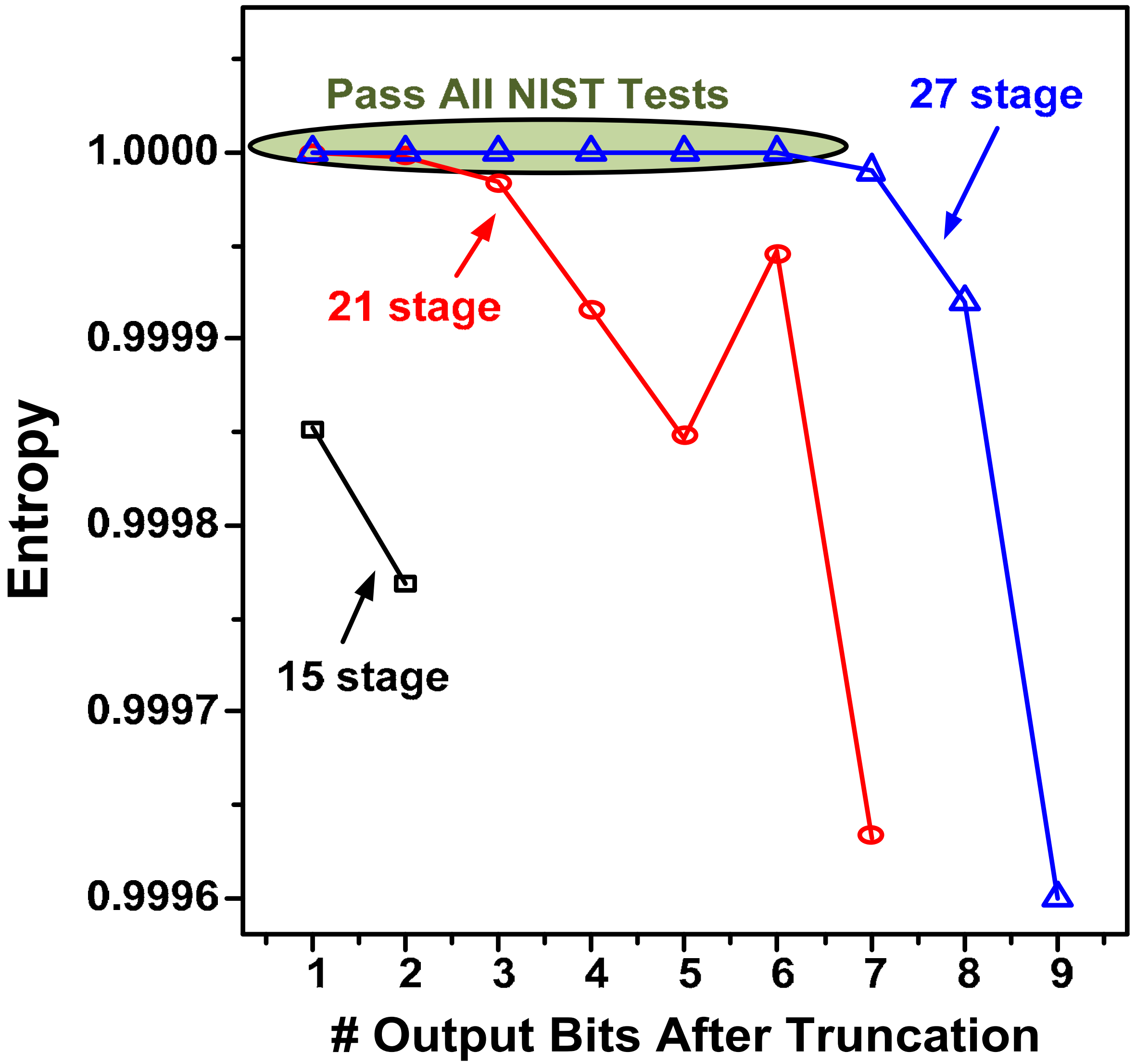
Impact of RO Length

- 65nm chip, VDD=1V



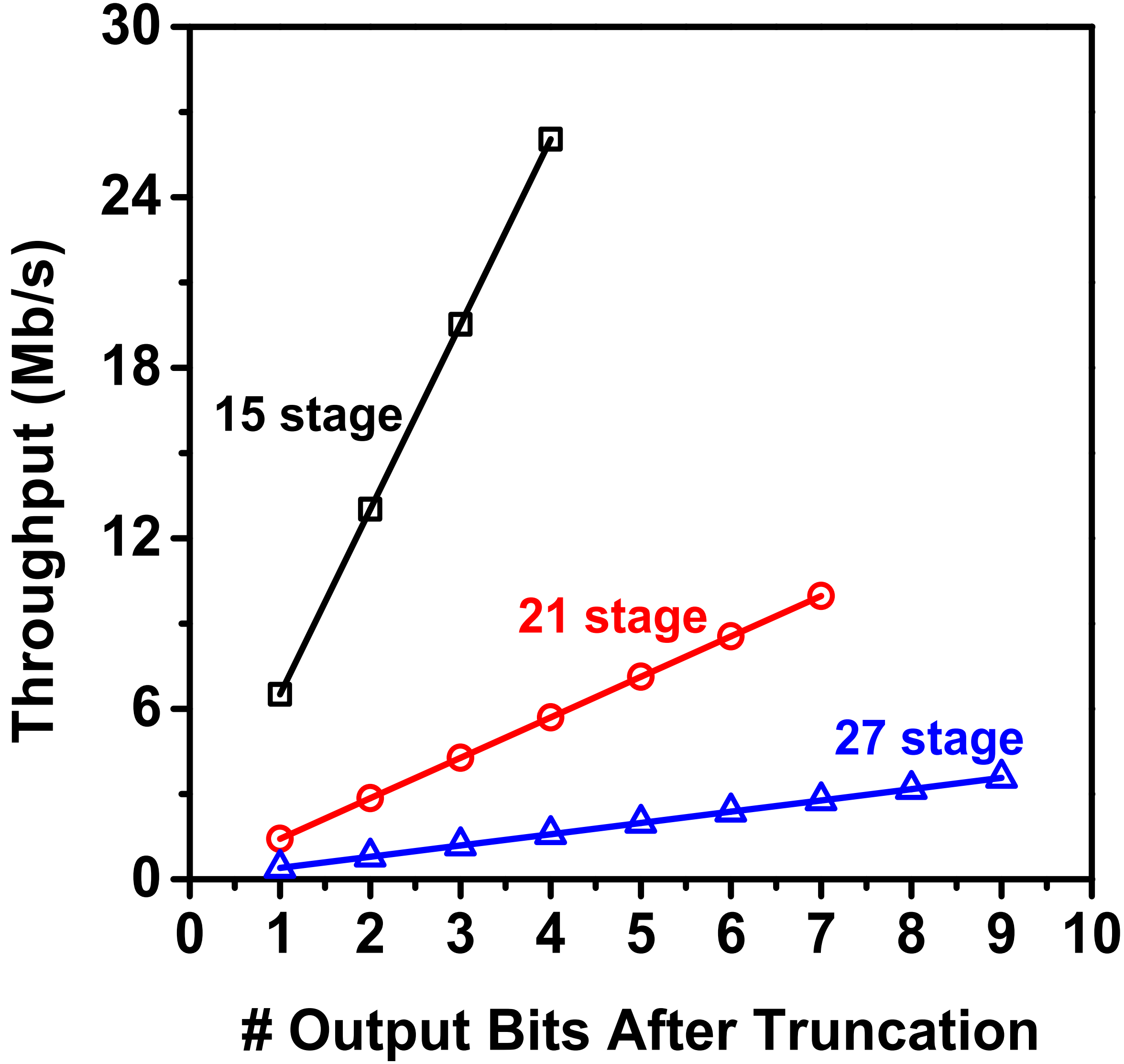
Impact of RO Length

- 65nm chip, VDD=1V



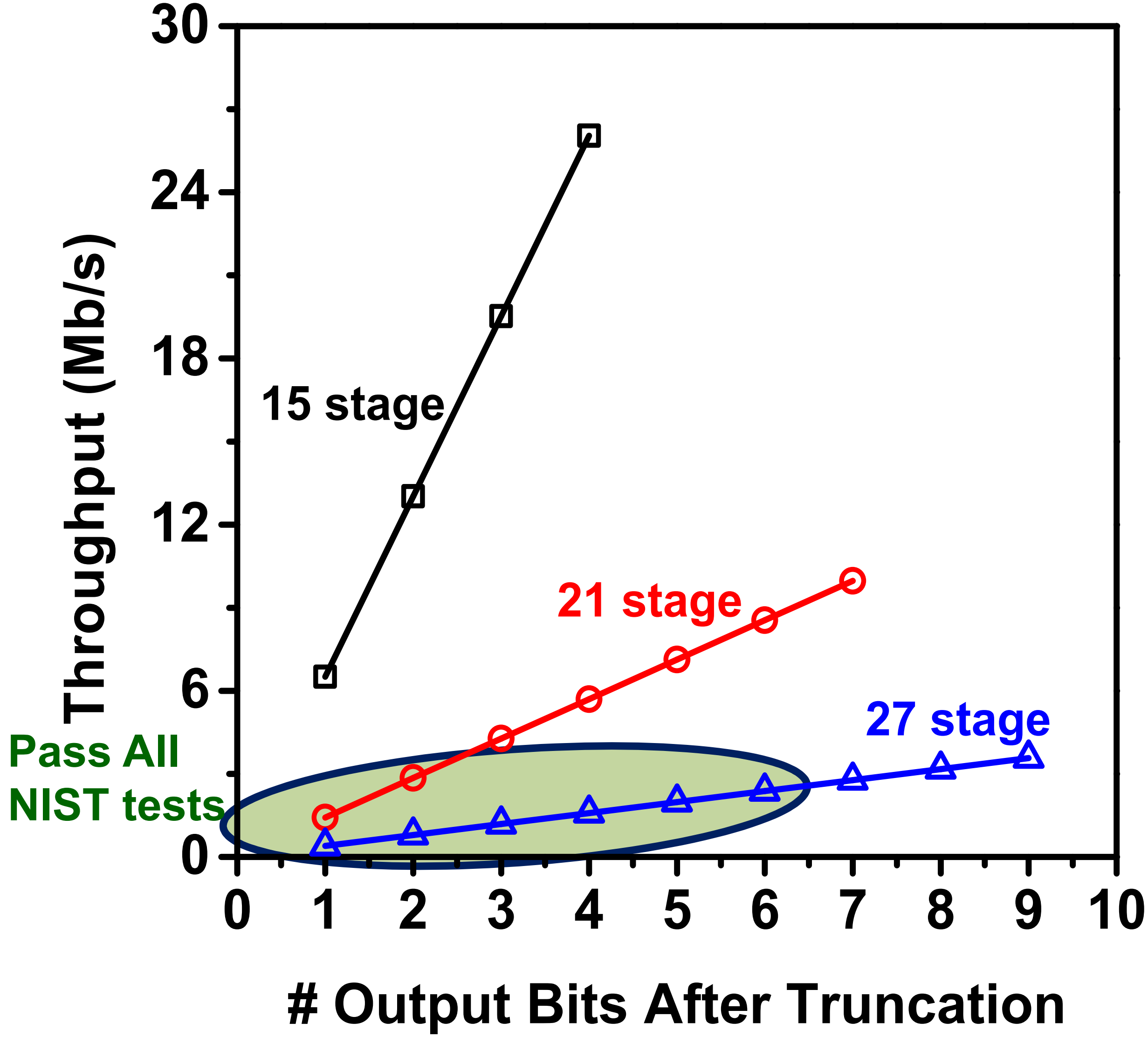
Impact of RO Length

- 65nm chip, VDD=1V



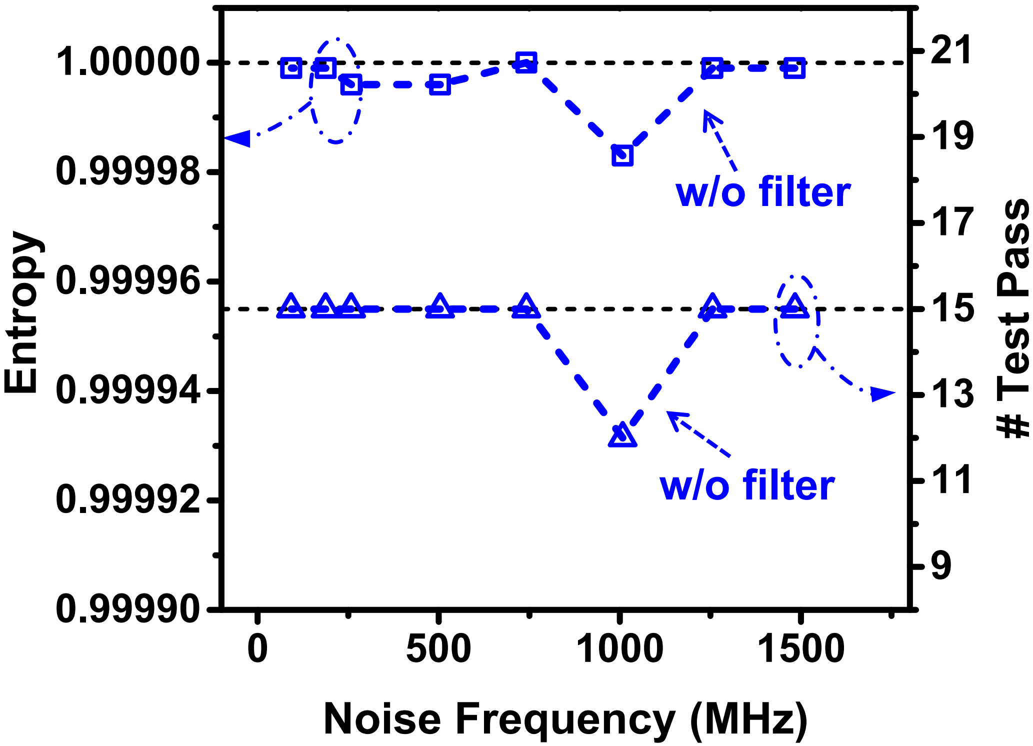
Impact of RO Length

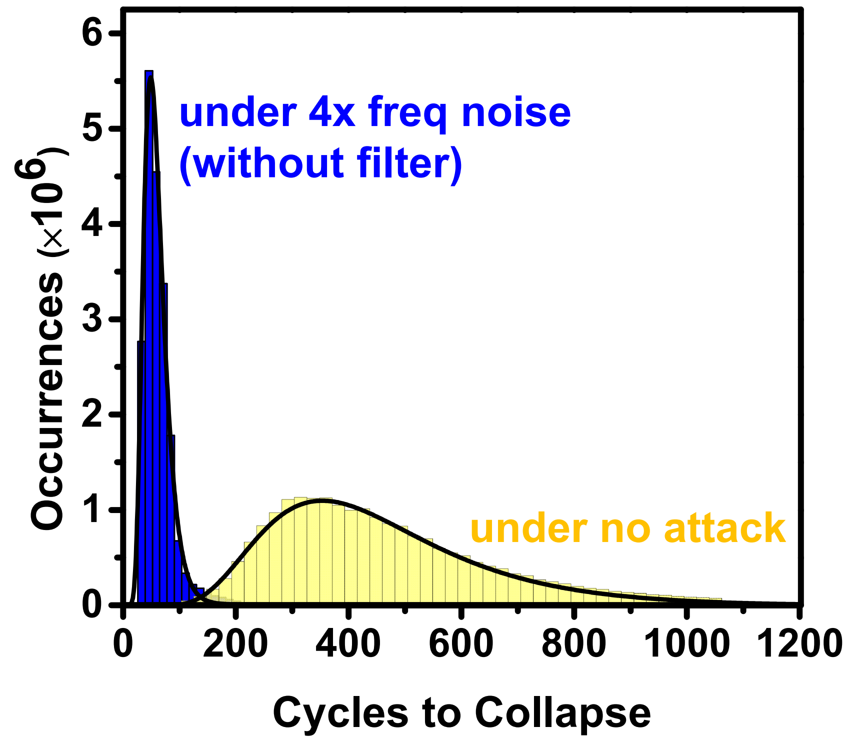
- 65nm chip, VDD=1V



Impact of On-Chip Noise

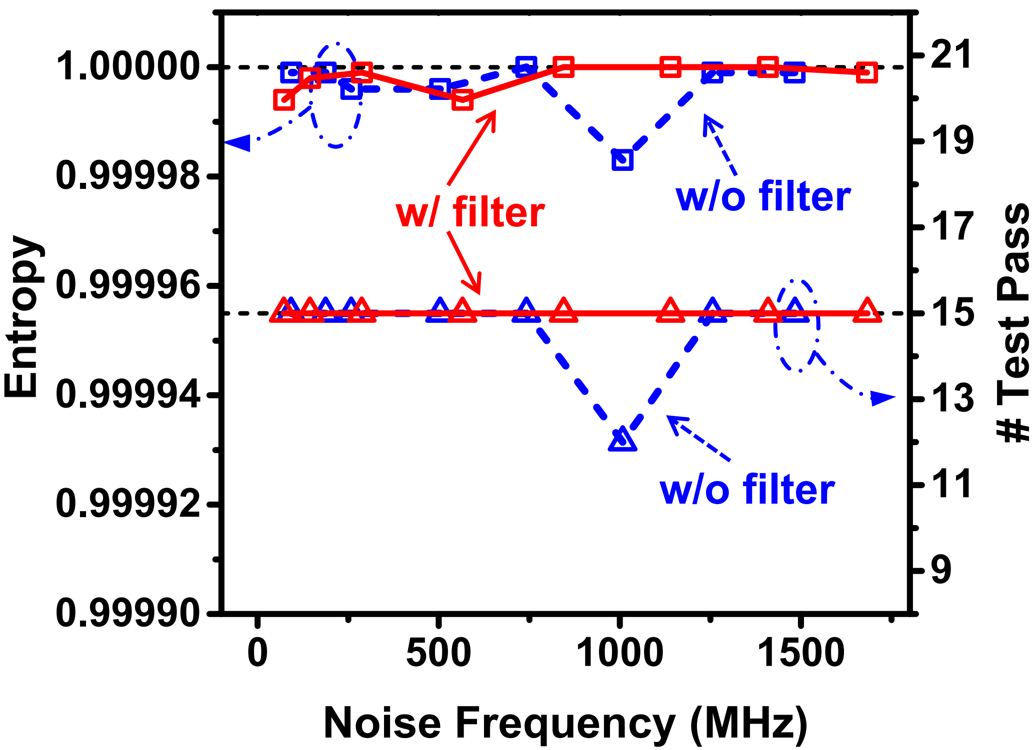
- 65nm chip, injected noise amplitude = 200mV
- Protected and unprotected TRNGs

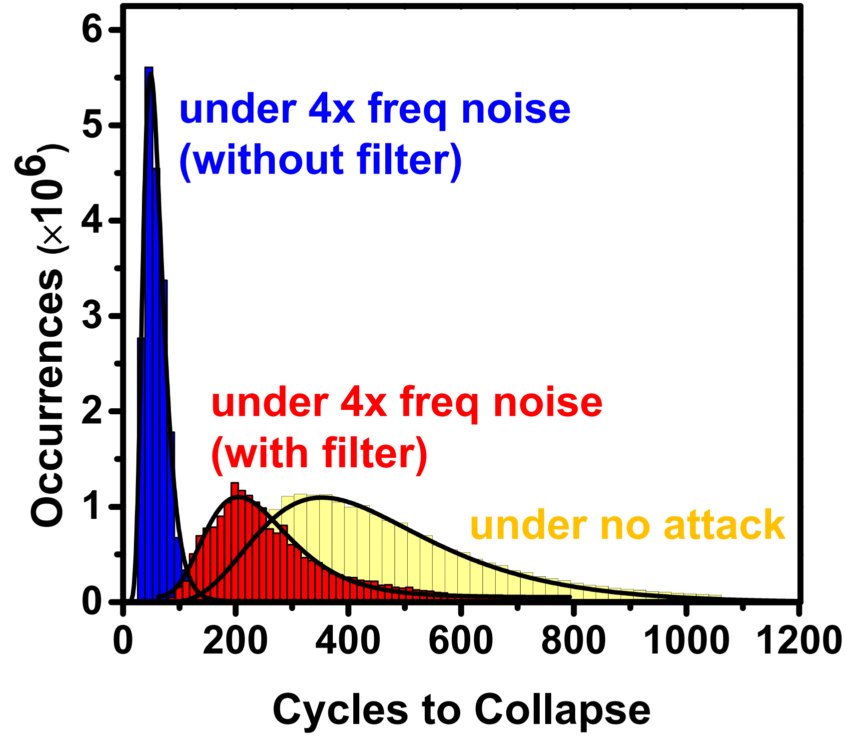




Impact of On-Chip Noise

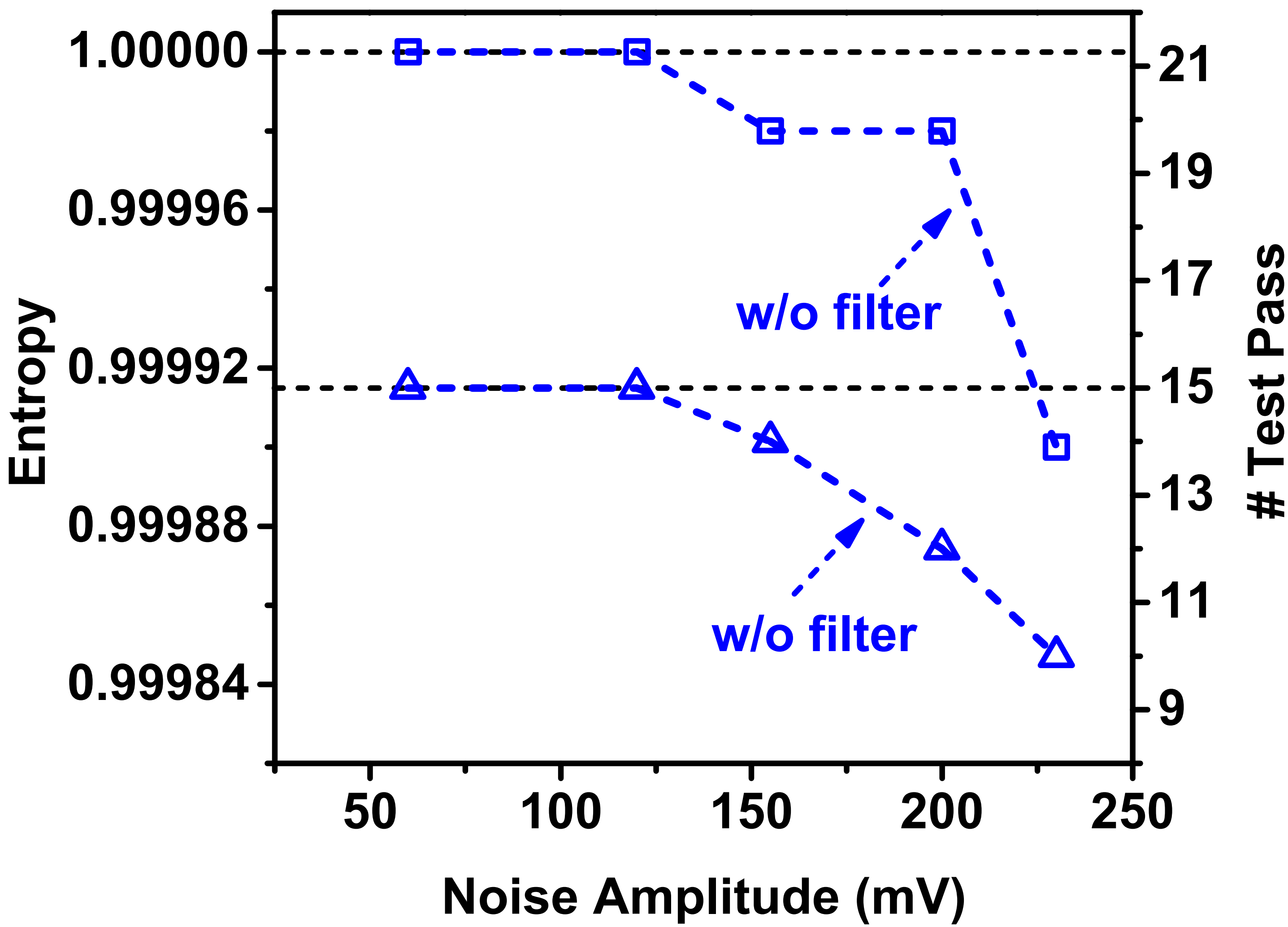
- 65nm chip, injected noise amplitude = 200mV
- Protected and unprotected TRNGs





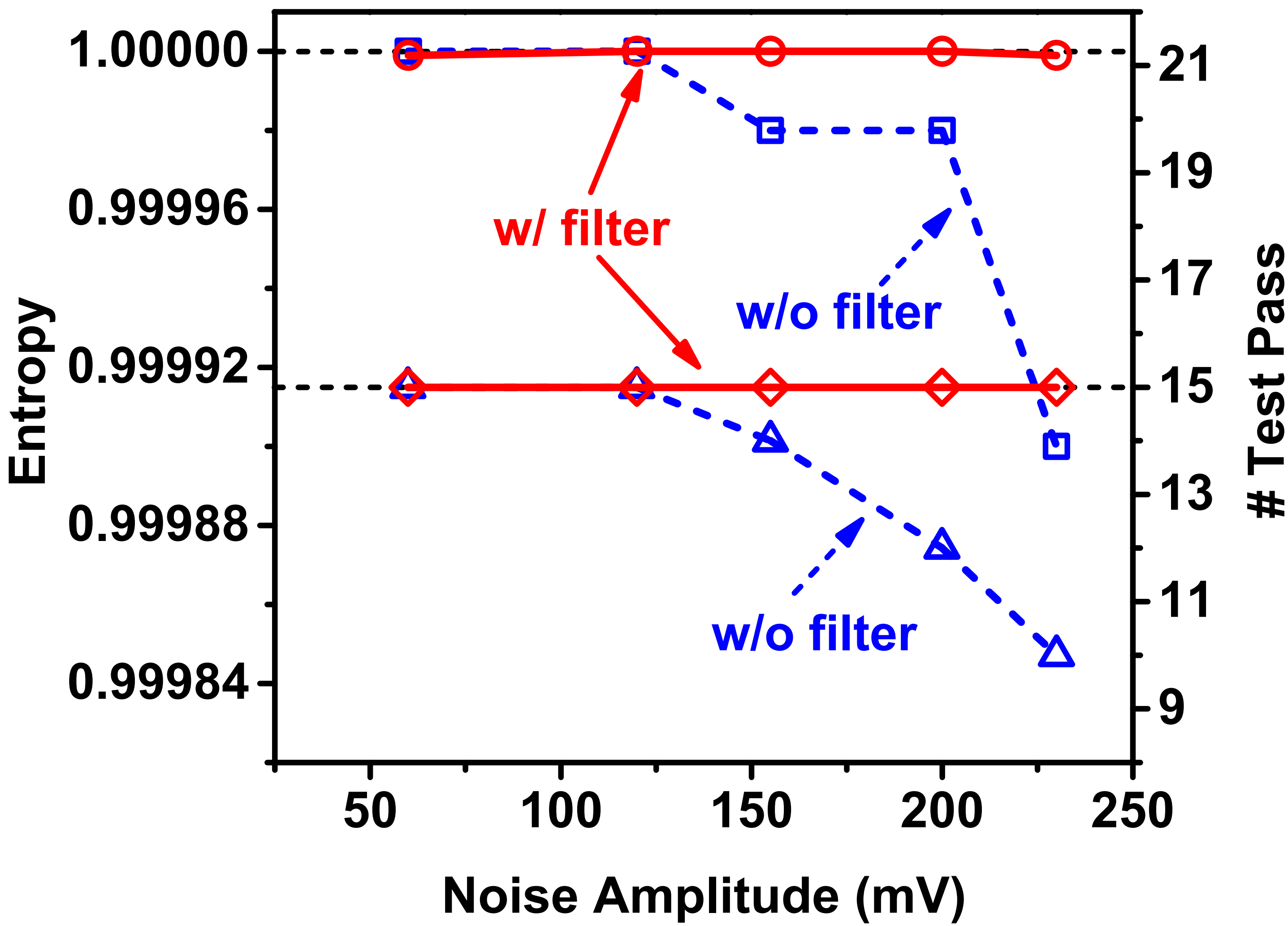
Impact of On-Chip Noise

- 65nm chip, injected noise freq = 4x nominal freq (worst case)



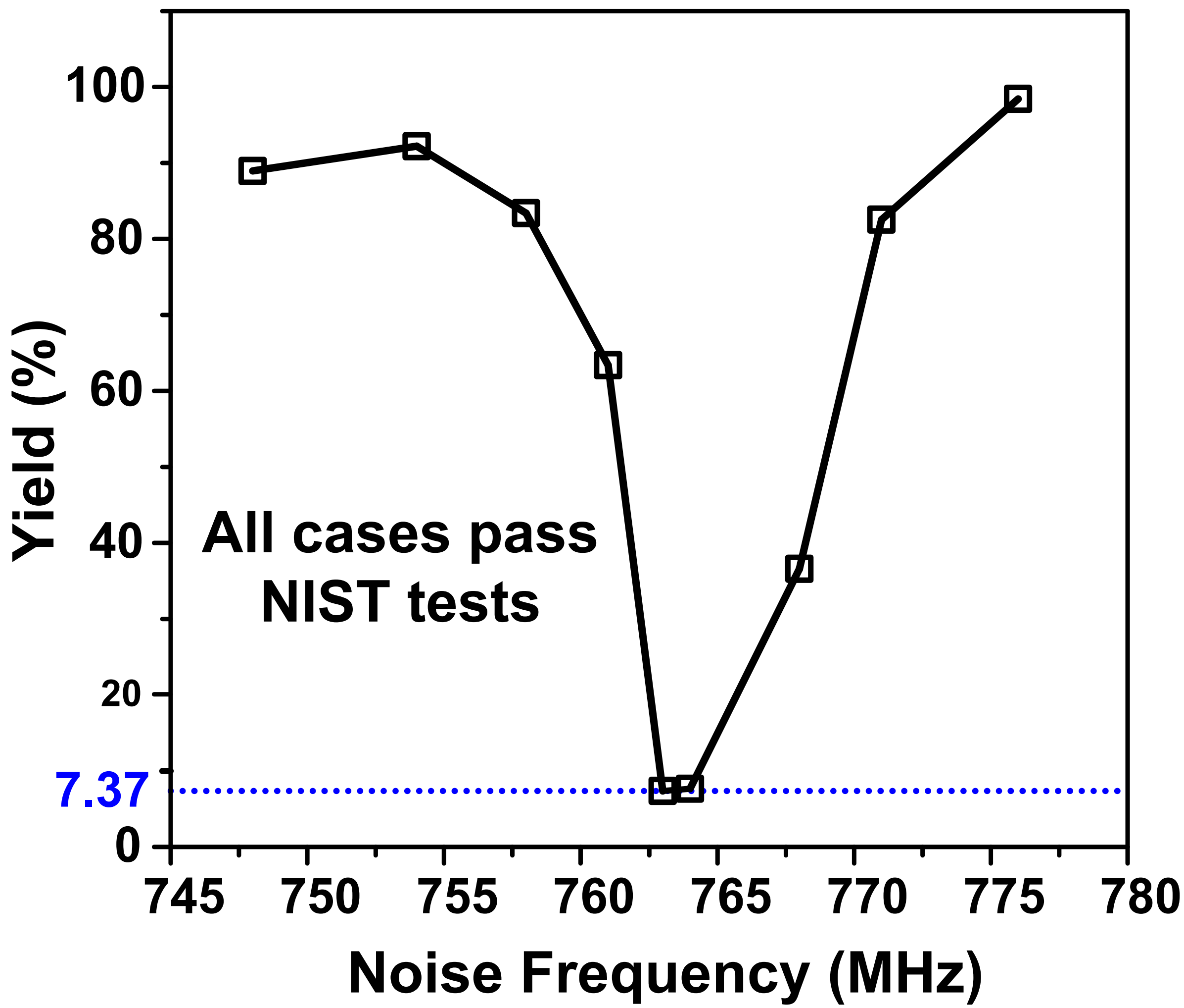
Impact of On-Chip Noise

- 65nm chip, injected noise freq = 4x nominal freq (worst case)

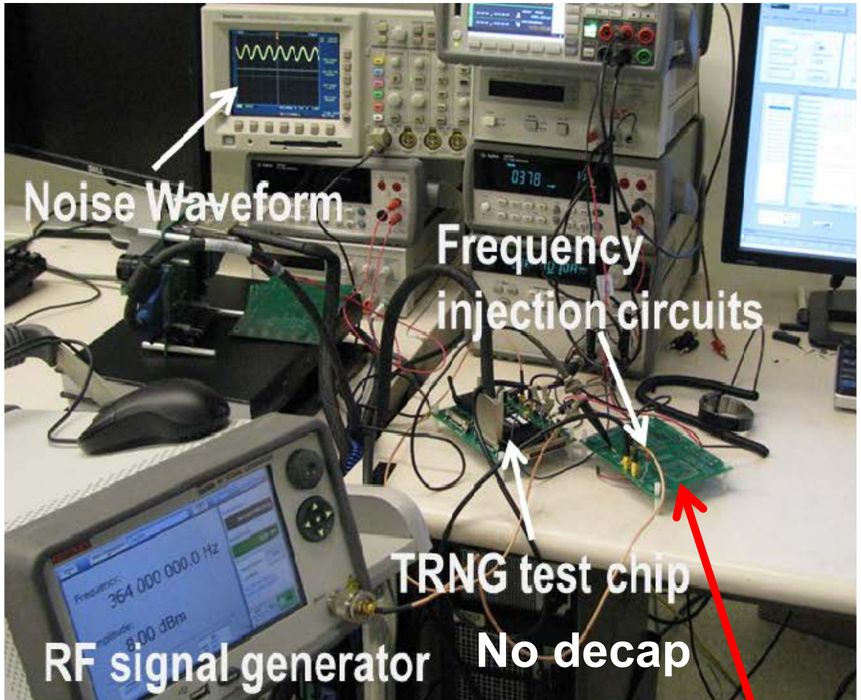


Denial of Service (DOS)

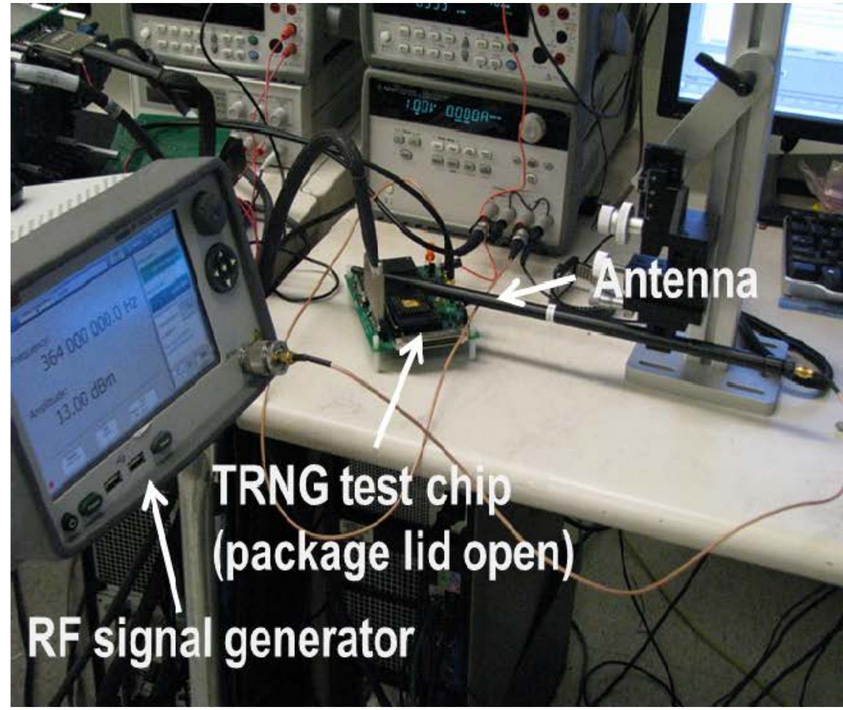
- Yield reduced to 7.37% under 3x frequency on-chip noise
- Randomness maintained



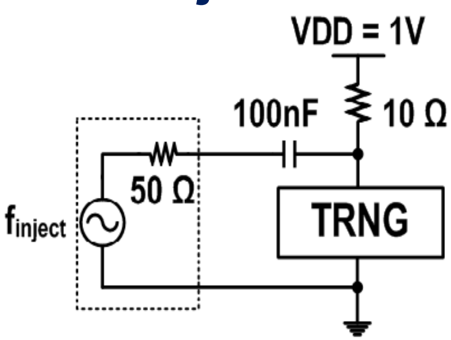
External Noise Injection



(1) Supply noise injection



(2) EM noise injection



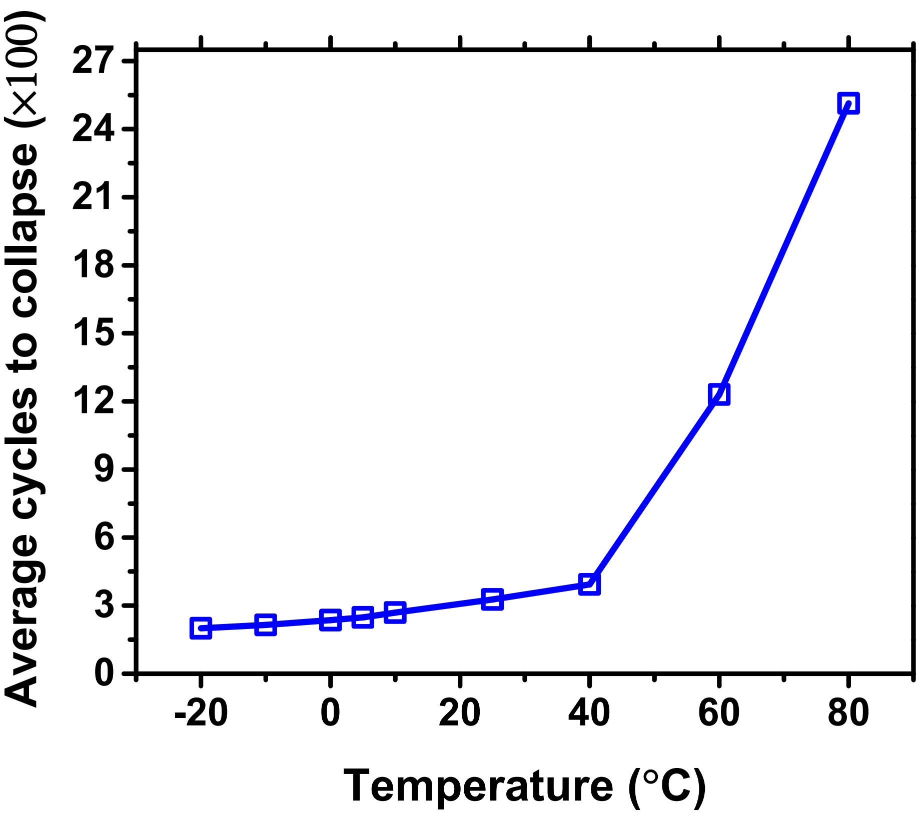
Frequency Injection Circuits

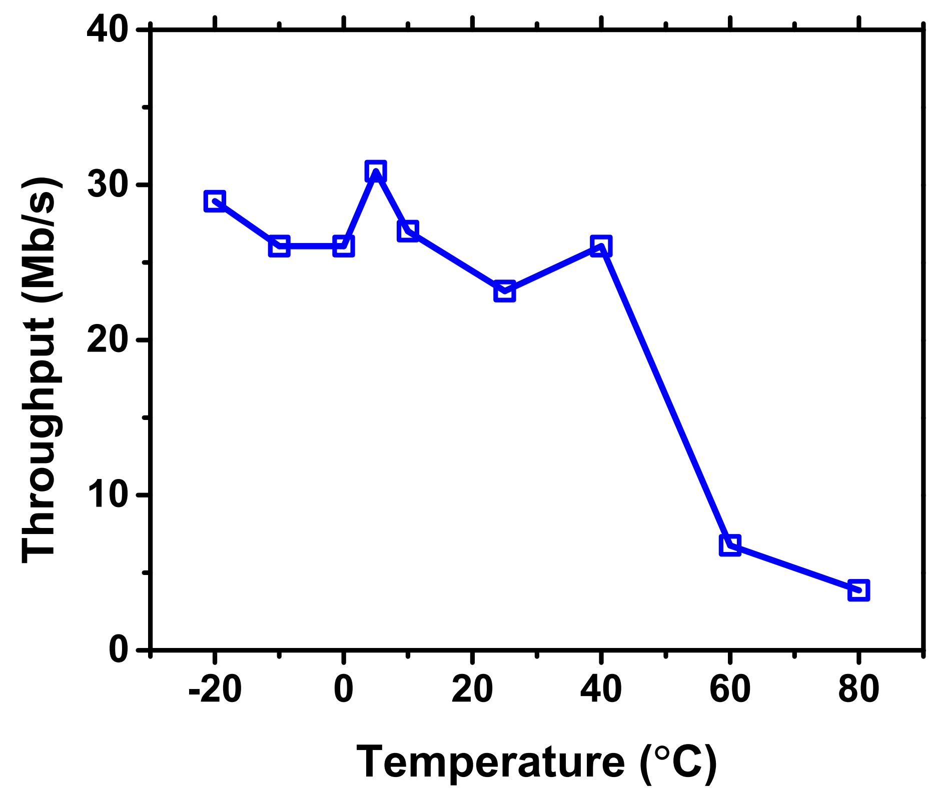
- **Both 28nm and 65nm chip consistently pass all NIST tests under these external noise injection tests up to power limit of signal generator**

Ref: A. Markettos, CHES, 2009

Temperature Sensitivity

- 28nm chip pass all 15 NIST tests from -20 °C to 80 °C
- Lower temp ⇨ narrower distribution, faster collapse
- Higher temp ⇨ wider distribution, slower collapse





Comparison Table

	This work (25°C, 0.9V core supply)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers' 03 [1]
Technology	**28nm**	**65nm**	45nm	65nm	0.25μm	0.13μm	0.12μm	0.18μm
Entropy Source	**Jitter in 3-edge RO**		Metas-tability	Oxide breakdown	SiN MOS-FET Noise	Metas-tability	Oxide traps	Oscillator jitter
Design Method	**Synthesized**		Custom digital	Custom digital	Custom analog	Custom digital	Custom analog	All digital
Bit Rate (Mb/s)	**23.16**	**2.8**	2400	0.011	2	0.2	0.2	10
NIST Pass	**All**	**All**	All	All	not reported[b]	5	not reported	not reported[b]
TRNG Core Area (μm²)	**375**	**960 (1080[a])**	4004	1200	1200	36300	9000	16000
Power (mW)	**0.54**	**0.159**	7	2	1.9	1	0.05	2.3
Efficiency (nJ/bit)	**0.023**	**0.057**	0.0029	181.81	0.95	5	0.25	0.23
Post Processing	**No**	**No**	No	No	Yes	No	Yes	no
Resistance to Attack	**Yes**	**Yes**	Not reported	Not reported	Not reported	Not reported	Not reported	No[c]

* Including 1/8th of filter area (MIM cap and poly resistor), filter is shared by 8 TRNG here and placed beneath the MIM cap.

** Only the given number of NIST test results are reported

*** Only NIST FIPS 140-2 test result is provided, which is out dated, less strict and requires only 20,000 bits compared to NIST Pub 800-22

Comparison Table

	This work (25°C, 0.9V core supply)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers' 03 [1]
Technology	**28nm**	**65nm**	45nm	65nm	0.25μm	0.13μm	0.12μm	0.18μm
Entropy Source	**Jitter in 3-edge RO**		Metas-tability	Oxide breakdown	SiN MOS-FET Noise	Metas-tability	Oxide traps	Oscillator jitter
Design Method	**Synthesized**		Custom digital	Custom digital	Custom analog	Custom digital	Custom analog	All digital
Bit Rate (Mb/s)	**23.16**	**2.8**	2400	0.011	2	0.2	0.2	10
NIST Pass	**All**	**All**	All	All	not reported[b]	5	not reported	not reported[b]
TRNG Core Area (μm^2)	**375**	**960 (1080[a])**	4004	1200	1200	36300	9000	16000
Power (mW)	**0.54**	**0.159**	7	2	1.9	1	0.05	2.3
Efficiency (nJ/bit)	**0.023**	**0.057**	0.0029	181.81	0.95	5	0.25	0.23
Post Processing	**No**	**No**	No	No	Yes	No	Yes	no
Resistance to Attack	**Yes**	**Yes**	Not reported	Not reported	Not reported	Not reported	Not reported	No[c]

* Including 1/8th of filter area (MIM cap and poly resistor), filter is shared by 8 TRNG here and placed beneath the MIM cap.

** Only the given number of NIST test results are reported

*** Only NIST FIPS 140-2 test result is provided, which is out dated, less strict and requires only 20,000 bits compared to NIST Pub 800-22

Comparison Table

	This work (25°C, 0.9V core supply)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers' 03 [1]
Technology	**28nm**	**65nm**	45nm	65nm	0.25µm	0.13µm	0.12µm	0.18µm
Entropy Source	**Jitter in 3-edge RO**		Metas-tability	Oxide breakdown	SiN MOS-FET Noise	Metas-tability	Oxide traps	Oscillator jitter
Design Method	**Synthesized**		Custom digital	Custom digital	Custom analog	Custom digital	Custom analog	All digital
Bit Rate (Mb/s)	**23.16**	**2.8**	2400	0.011	2	0.2	0.2	10
NIST Pass	**All**	**All**	All	All	not reported[b]	5	not reported	not reported[b]
TRNG Core Area (μm^2)	**375**	**960 (1080[a])**	4004	1200	1200	36300	9000	16000
Power (mW)	**0.54**	**0.159**	7	2	1.9	1	0.05	2.3
Efficiency (nJ/bit)	**0.023**	**0.057**	0.0029	181.81	0.95	5	0.25	0.23
Post Processing	**No**	**No**	No	No	Yes	No	Yes	no
Resistance to Attack	**Yes**	**Yes**	Not reported	Not reported	Not reported	Not reported	Not reported	No[c]

* Including 1/8th of filter area (MIM cap and poly resistor), filter is shared by 8 TRNG here and placed beneath the MIM cap.

** Only the given number of NIST test results are reported

*** Only NIST FIPS 140-2 test result is provided, which is out dated, less strict and requires only 20,000 bits compared to NIST Pub 800-22

Comparison Table

	This work (25°C, 0.9V core supply)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers' 03 [1]
Technology	**28nm**	**65nm**	45nm	65nm	0.25µm	0.13µm	0.12µm	0.18µm
Entropy Source	**Jitter in 3-edge RO**		Metas-tability	Oxide breakdown	SiN MOS-FET Noise	Metas-tability	Oxide traps	Oscillator jitter
Design Method	**Synthesized**		Custom digital	Custom digital	Custom analog	Custom digital	Custom analog	All digital
Bit Rate (Mb/s)	**23.16**	**2.8**	2400	0.011	2	0.2	0.2	10
NIST Pass	**All**	**All**	All	All	not reported[b]	5	not reported	not reported[b]
TRNG Core Area (µm²)	**375**	**960 (1080[a])**	4004	1200	1200	36300	9000	16000
Power (mW)	**0.54**	**0.159**	7	2	1.9	1	0.05	2.3
Efficiency (nJ/bit)	**0.023**	**0.057**	0.0029	181.81	0.95	5	0.25	0.23
Post Processing	**No**	**No**	No	No	Yes	No	Yes	no
Resistance to Attack	**Yes**	**Yes**	Not reported	Not reported	Not reported	Not reported	Not reported	No[c]

* Including 1/8th of filter area (MIM cap and poly resistor), filter is shared by 8 TRNG here and placed beneath the MIM cap.

** Only the given number of NIST test results are reported

*** Only NIST FIPS 140-2 test result is provided, which is out dated, less strict and requires only 20,000 bits compared to NIST Pub 800-22

Comparison Table

	This work (25°C, 0.9V core supply)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers' 03 [1]
Technology	**28nm**	**65nm**	45nm	65nm	0.25µm	0.13µm	0.12µm	0.18µm
Entropy Source	**Jitter in 3-edge RO**		Metas-tability	Oxide breakdown	SiN MOS-FET Noise	Metas-tability	Oxide traps	Oscillator jitter
Design Method	**Synthesized**		Custom digital	Custom digital	Custom analog	Custom digital	Custom analog	All digital
Bit Rate (Mb/s)	**23.16**	**2.8**	2400	0.011	2	0.2	0.2	10
NIST Pass	**All**	**All**	All	All	not reported[b]	5	not reported	not reported[b]
TRNG Core Area (µm²)	**375**	**960 (1080[a])**	4004	1200	1200	36300	9000	16000
Power (mW)	**0.54**	**0.159**	7	2	1.9	1	0.05	2.3
Efficiency (nJ/bit)	**0.023**	**0.057**	0.0029	181.81	0.95	5	0.25	0.23
Post Processing	**No**	**No**	No	No	Yes	No	Yes	no
Resistance to Attack	**Yes**	**Yes**	Not reported	Not reported	Not reported	Not reported	Not reported	No[c]

* Including 1/8th of filter area (MIM cap and poly resistor), filter is shared by 8 TRNG here and placed beneath the MIM cap.

** Only the given number of NIST test results are reported

*** Only NIST FIPS 140-2 test result is provided, which is out dated, less strict and requires only 20,000 bits compared to NIST Pub 800-22

Conclusions

- A fully synthesized TRNG passing all NIST randomness tests fabricated in both 28nm and 65nm CMOS
- The TRNG harvests entropy from 3 edge ROs requiring no calibration or post-processing
- At 23.16Mb/s, it consumes 0.54mW and occupies 375μm^2 in 28nm
- Tolerance to power supply injection attack is verified by on-chip test structure as well as external noise injection. Resistance can be enhanced by noise filter

Columbia University
in the City of New York

0.6-1.0V, 279μm^2, 0.92μW Temperature Sensor with ≤+3.2/-3.4^{o}C Error for Dense On-Chip Thermal Monitoring

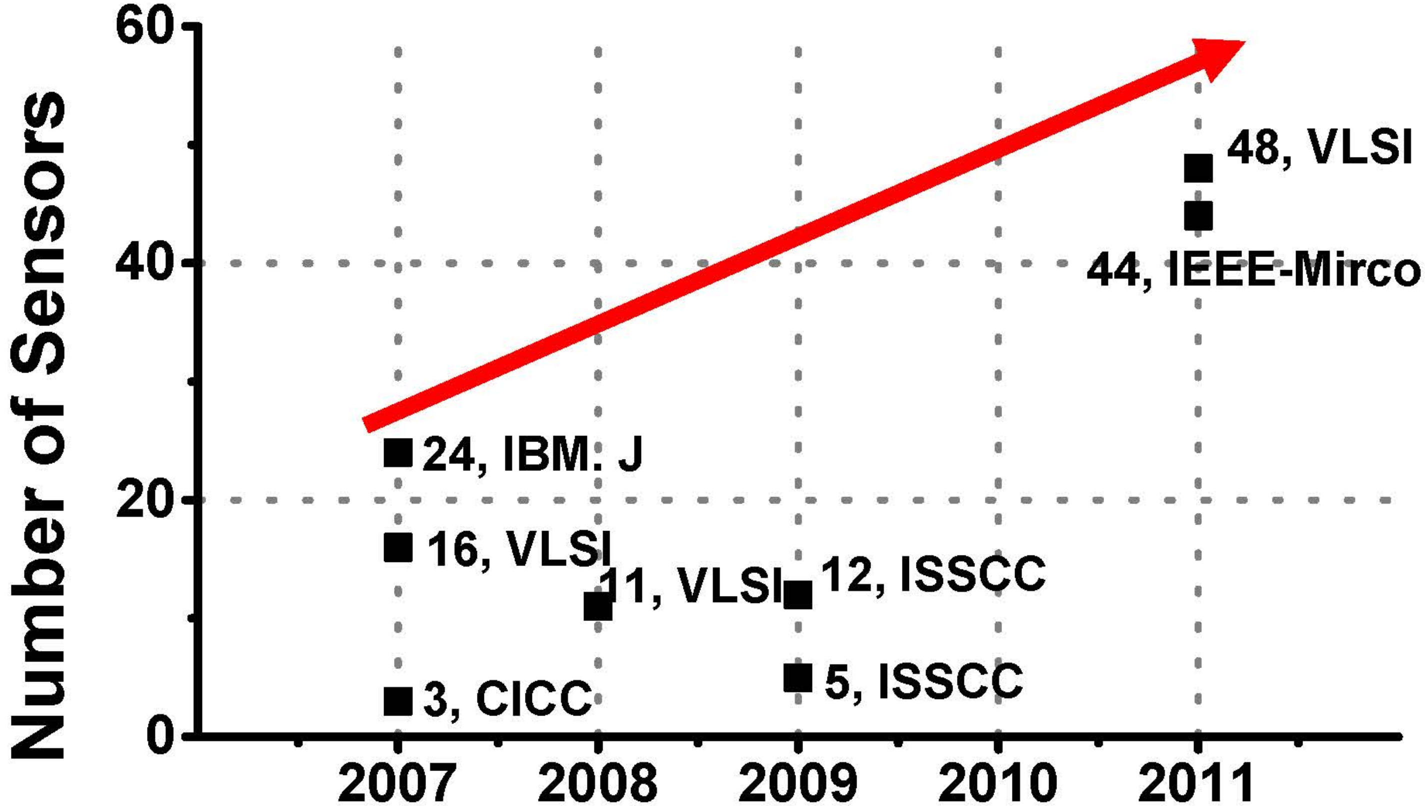
Teng Yang, Seongjong Kim,
Peter R. Kinget, Mingoo Seok

Columbia Integrated Systems Laboratory http://www.cisl.columbia.edu

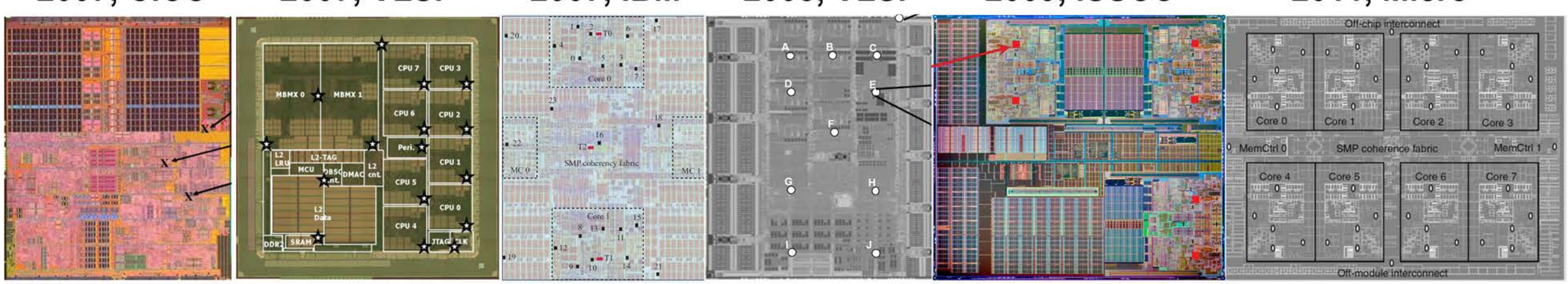
VLSI Lab at Columbia University

Analog & RF IC Design Research

Increasing Number of Sensors

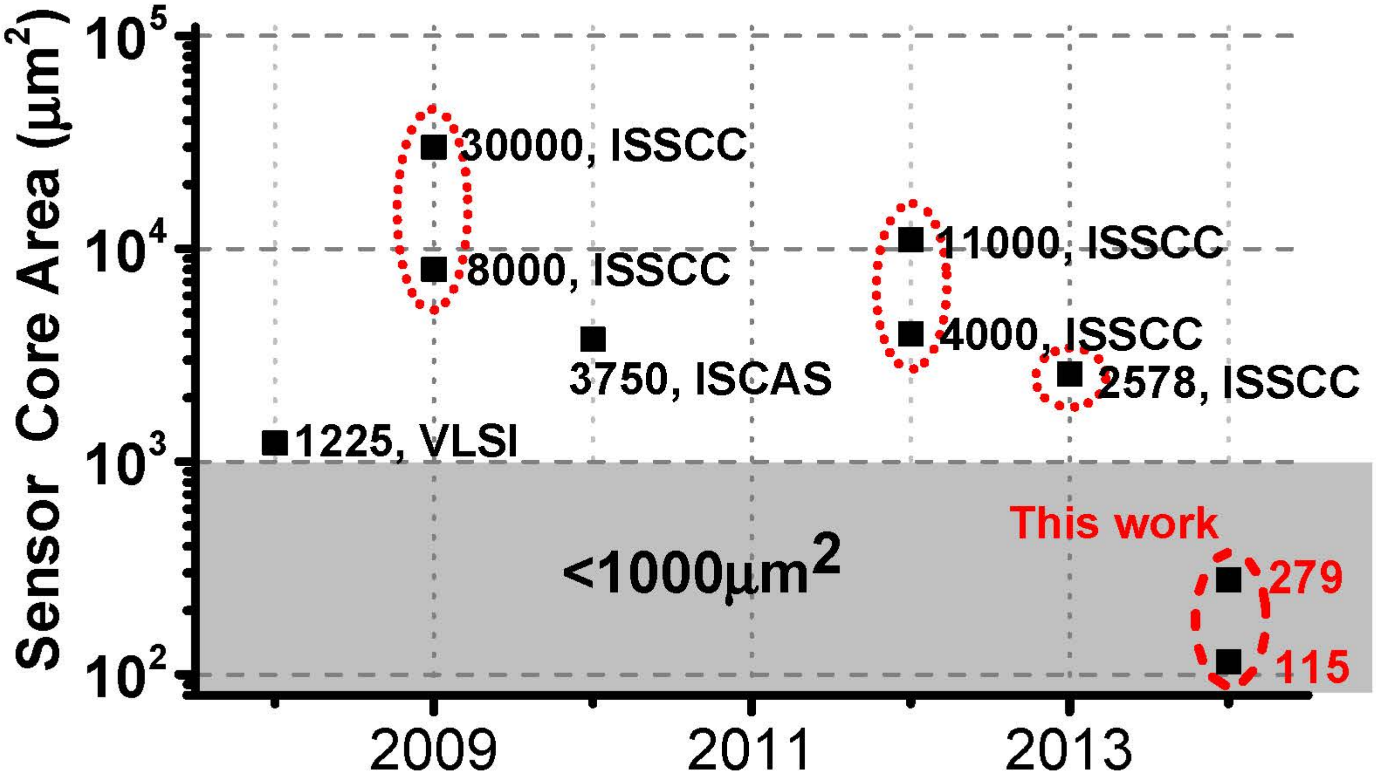


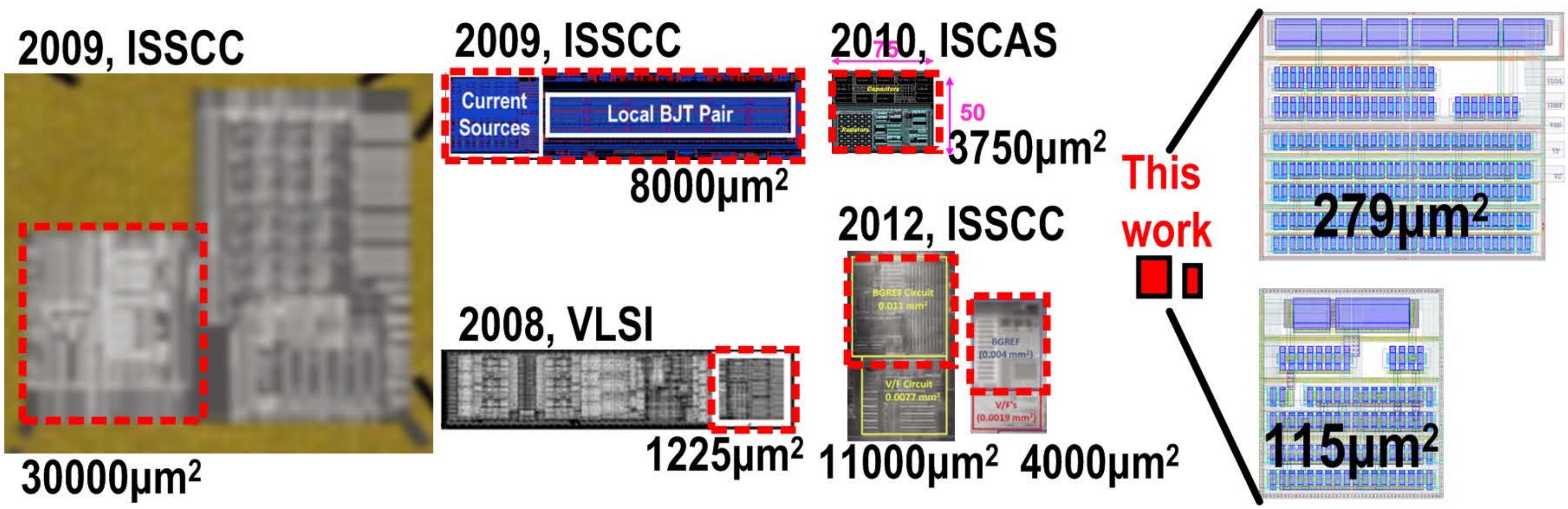
2007, CICC | 2007, VLSI | 2007, IBM | 2008, VLSI | 2009, ISSCC | 2011, Micro



3 | 16, 1/core | 24, 8/core | 11 | 12, 2/core | 44, 5/core

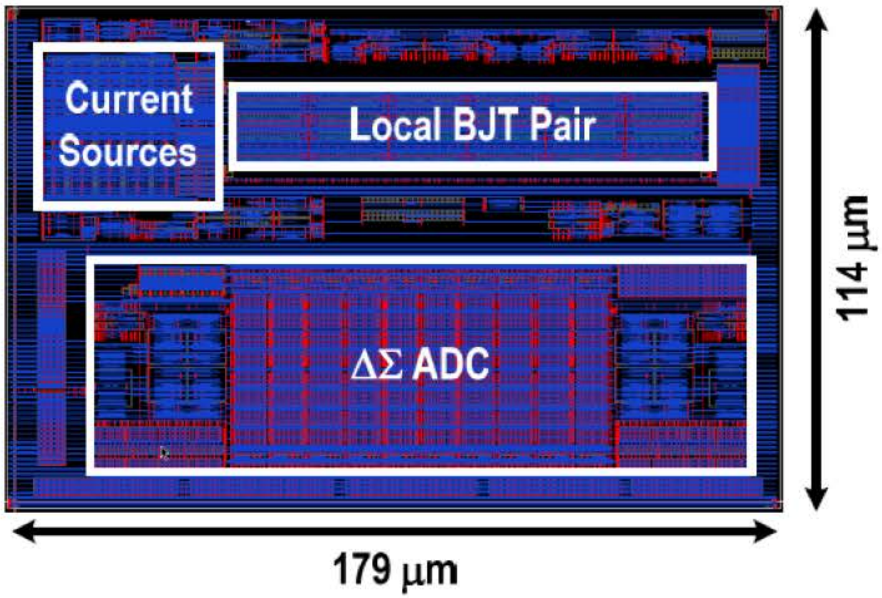
Sensor Core Area





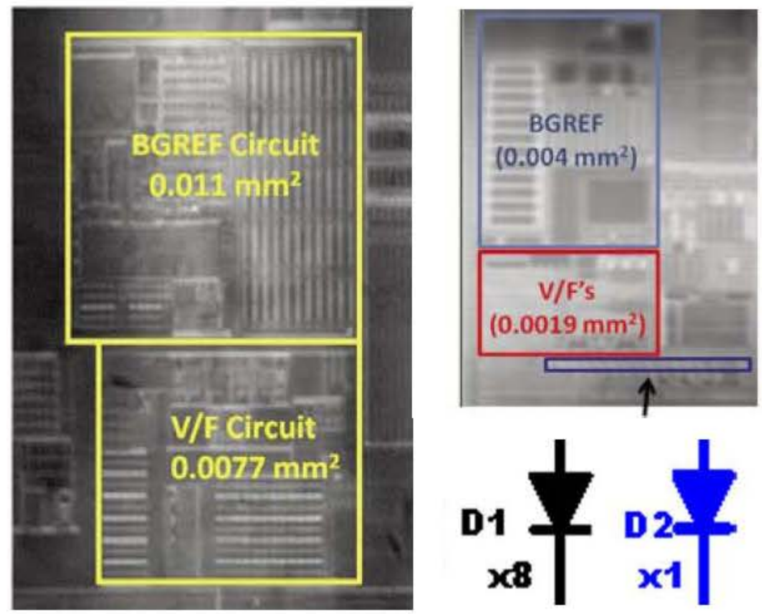
Related Work

[2] ISSCC, Y. W. Li, et al.



- <5°C accuracy w.o. cali.
- Sensor Core~8000µm^2
- V_{DD}=1.05V

[1] ISSCC, J. Shor, et al.



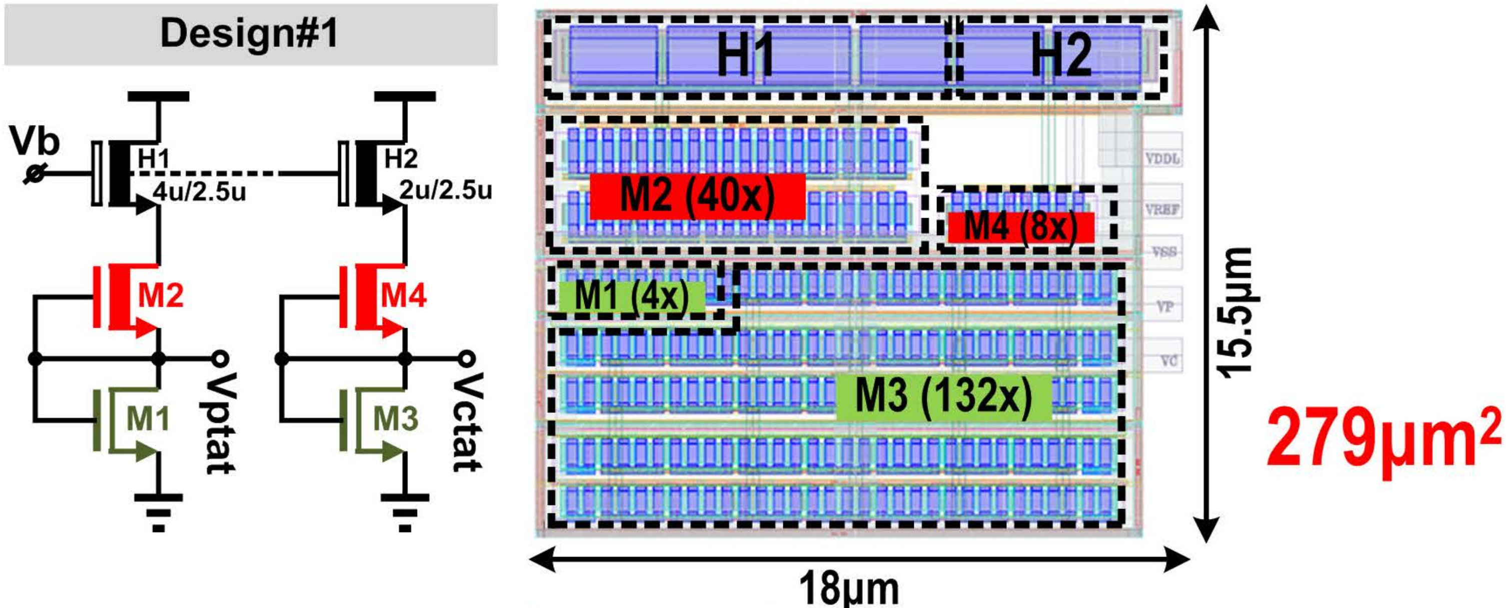
- <4.5°C accuracy w. OPC
- BGREF>4000µm^2
- V_{DD}>1.35V

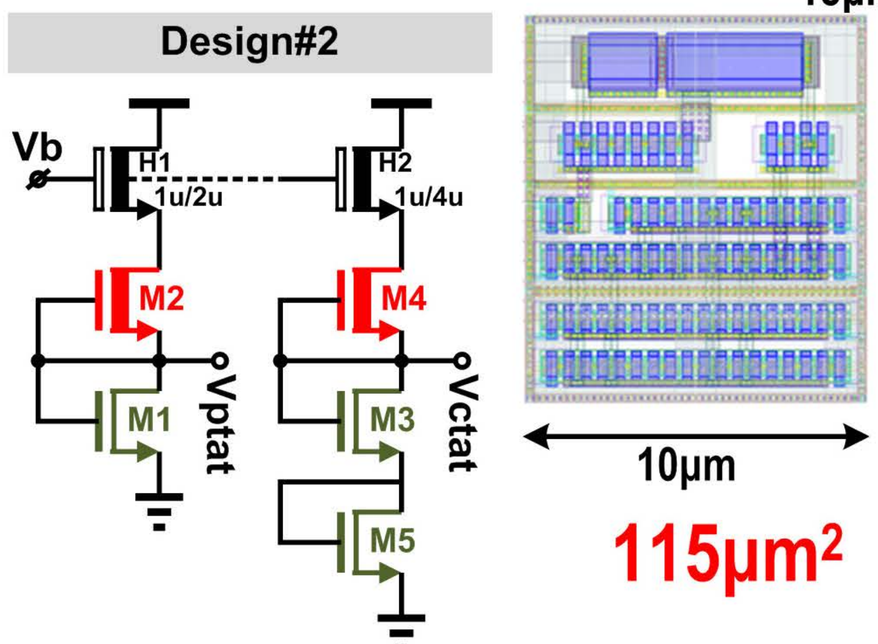
Overview of This Work

- Small area
- Supply Voltage Scalability

	Sensor #1	Sensor #2
Area	279μm^2	115μm^2
V_{DD} range	0.6~1.0V	
DC-PSRR	1.2^{o}C/V	0.8^{o}C/V

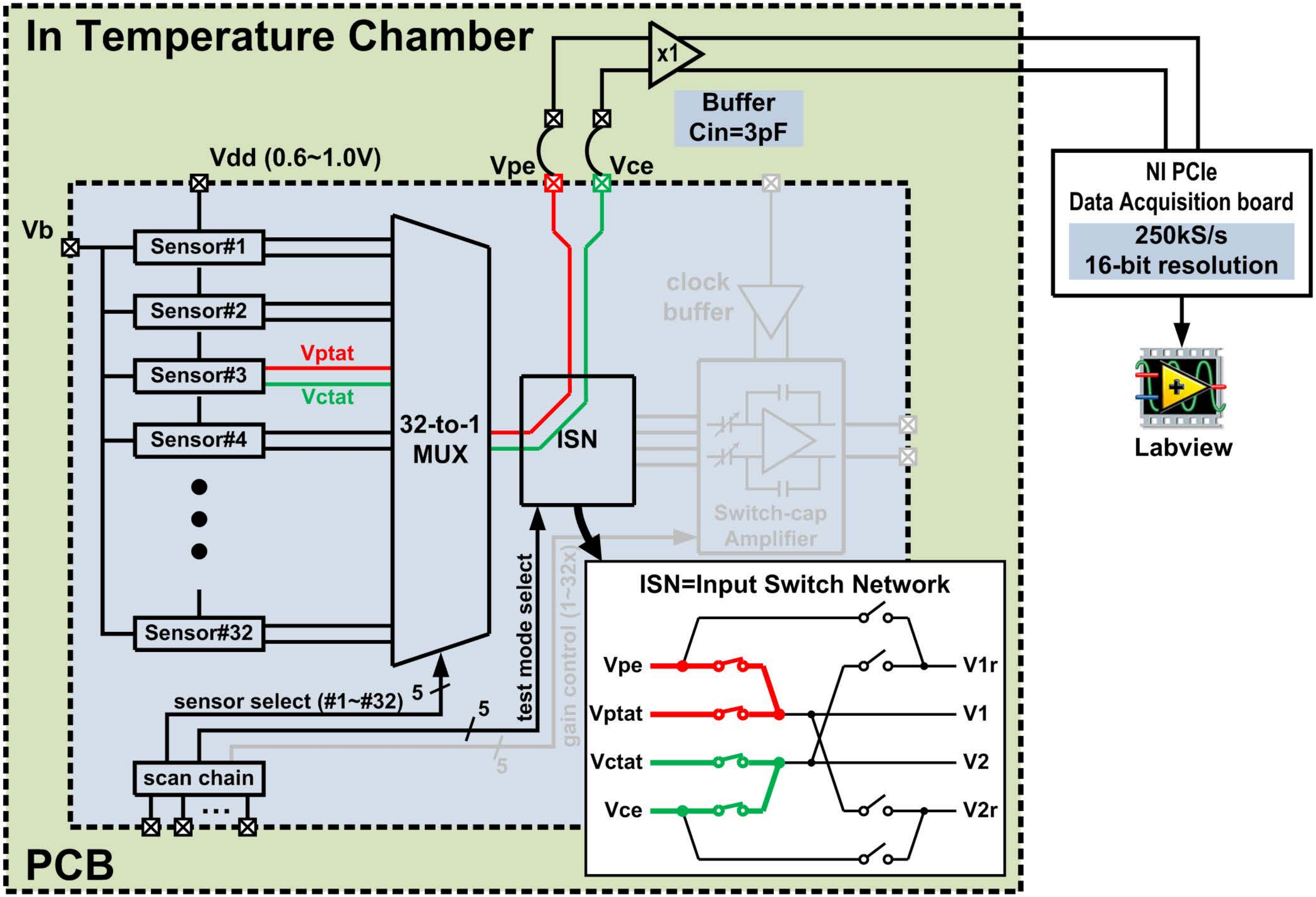
Overview of This Work





- Design #1: Area-Accuracy balanced
- Design #2: Area-optimized design

Test Chip Structure



Outline

I. Motivation and Design Overview
II. Design Approach
   1. Principles
   2. Challenge: Larger Temperature Sensitivity
   3. Challenge: Improve Accuracy
   4. Challenge: V_{DD} Scalability
III. Measurement summary and Comparisons
IV. Conclusion

Outline

I. Motivation and Design Overview

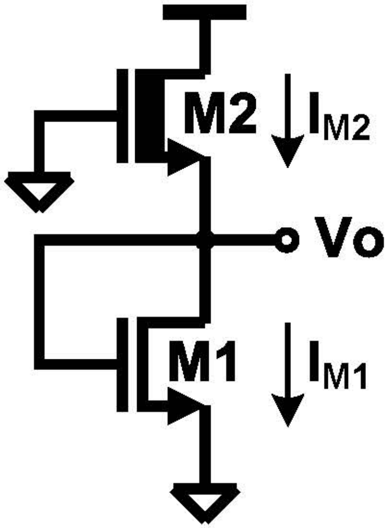
II. Design Approach

   1. Principles
   2. Challenge: Larger Temperature Sensitivity
   3. Challenge: Improve Accuracy
   4. Challenge: V_{DD} Scalability

III. Measurement summary and Comparisons

IV. Conclusion

Fundamental of the Proposed Sensors



- Sub-threshold region current

$$I_d = \mu C'_{ox}\frac{W}{L}(n-1)\phi_t^2 \cdot exp\left(\frac{V_{gs}-V_{th}}{n\phi_t}\right)\cdot\left[1-exp\left(-\frac{V_{ds}}{\phi_t}\right)\right]$$

- M1 and M2 work at a sub-threshold region

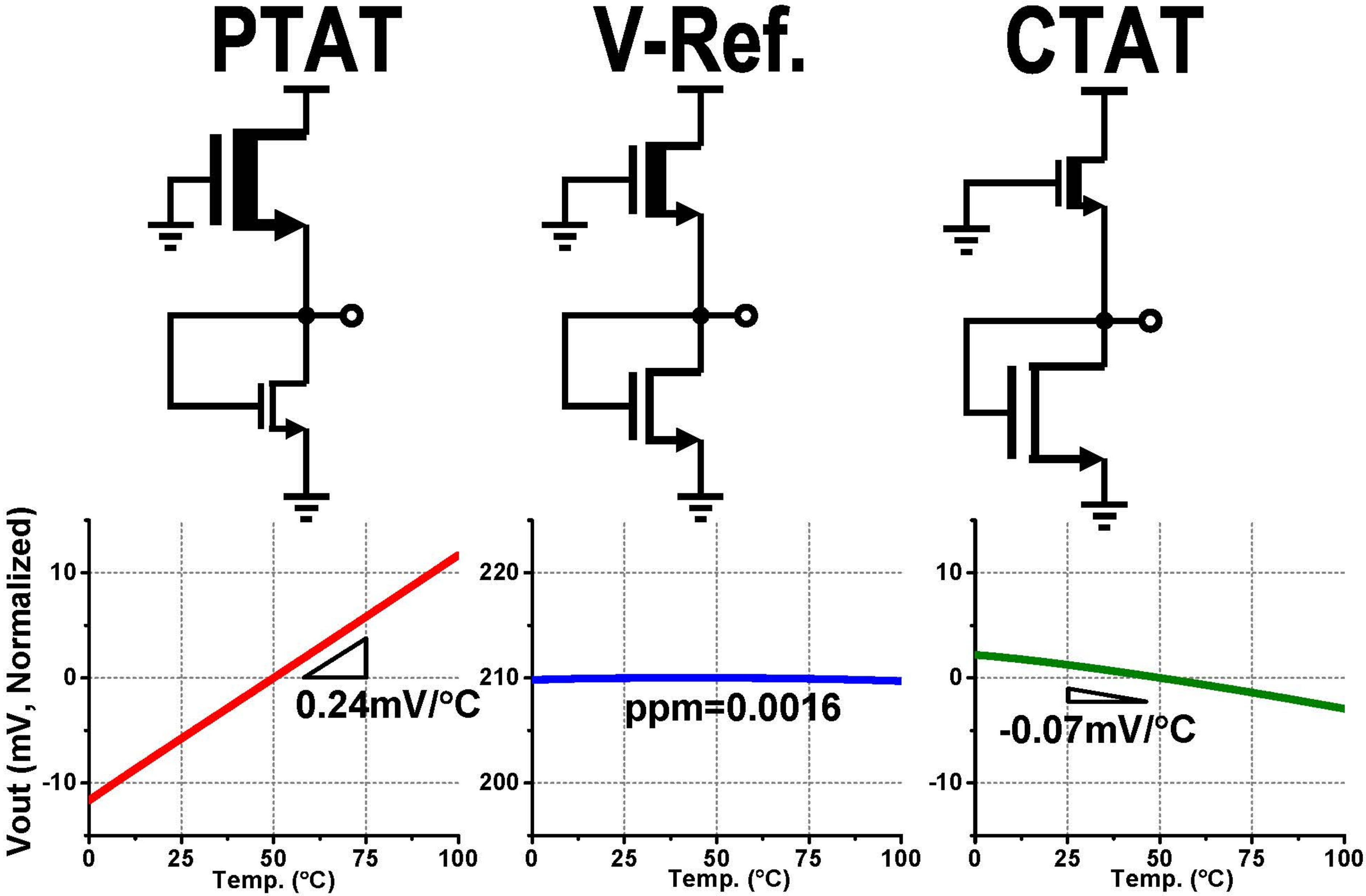
$$V_{out} = \boxed{\frac{n_1 n_2}{n_1+n_2}\ln\left(\frac{\mu_1}{\mu_2}\cdot\frac{C'_{ox1}}{C'_{ox2}}\cdot\frac{W_1 L_2}{W_2 L_1}\cdot\frac{n_1-1}{n_2-1}\right)\frac{k}{q}}\cdot T + \boxed{\frac{n_1 V_{th2} - n_2 V_{th1}}{n_1+n_2}}$$

offset~ΔVth

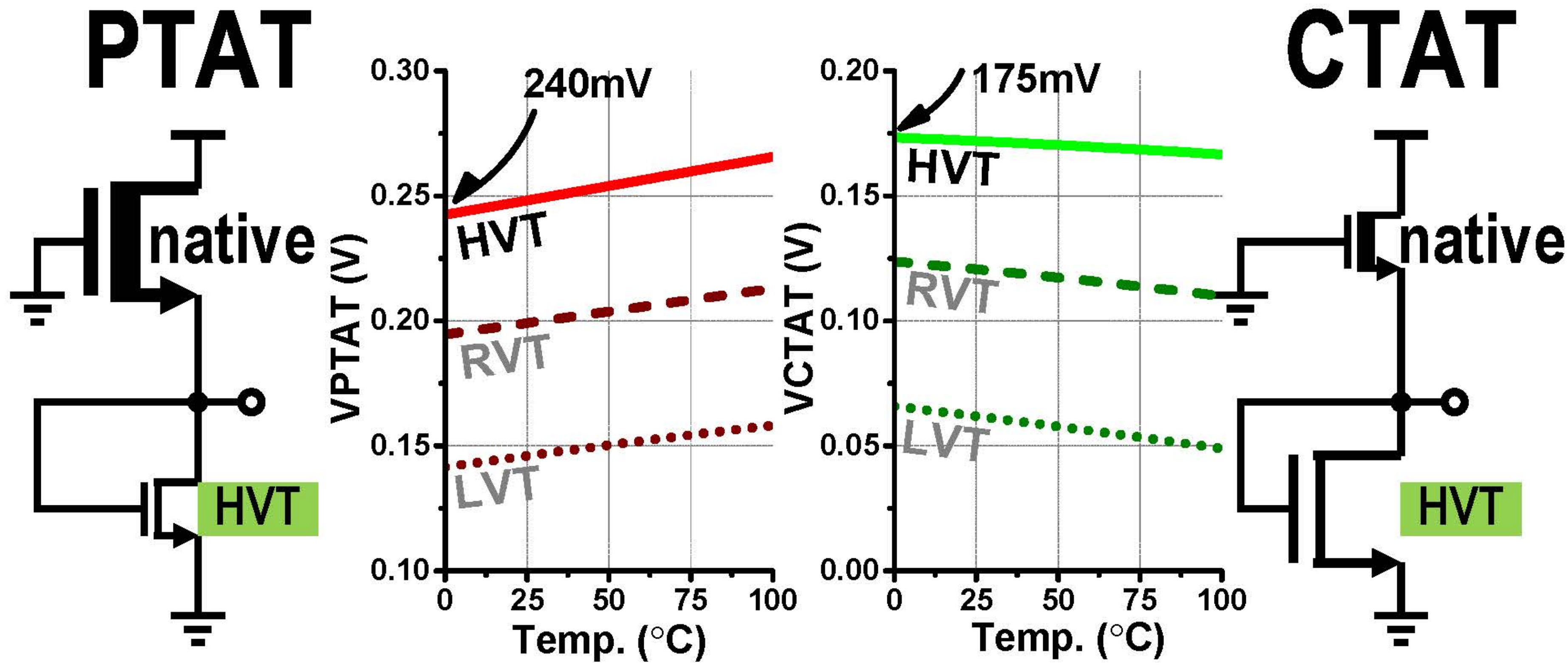
$$\boldsymbol{V_{out} = a \cdot T + b}$$

Modulate slope with **“Sizing Ratio”**	Tune offset with **“Device Type”**

Modulate Slopes with Sizing Ratio



Tune Offsets with Device Types



- Offset is determined by the V_{TH} difference
- Choose HVT: Ensure V_{DS}>>ϕ_t across 0°C~100°C

$$I_d = \mu C'_{ox}\frac{W}{L}(n-1)\phi_t^2 \cdot exp\left(\frac{V_{gs}-V_{th}}{n\phi_t}\right)\cdot\cancel{\left[\mathbf{1}-\boldsymbol{exp}\left(-\frac{\boldsymbol{V_{ds}}}{\boldsymbol{\phi_t}}\right)\right]}$$

Outline

I. Motivation and Design Overview

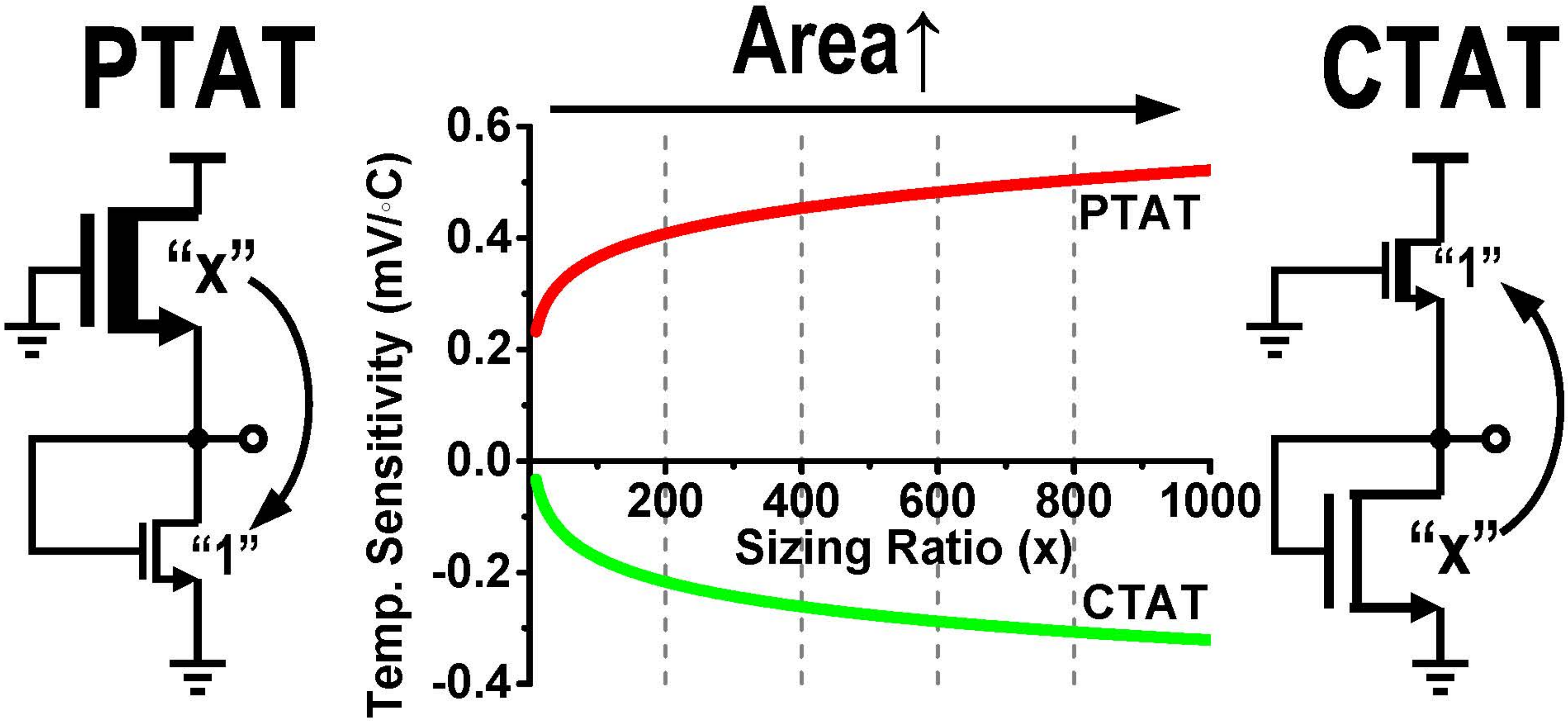
II. Design Approach

1. Principles
2. Challenge: Larger Temperature Sensitivity
3. Challenge: Improve Accuracy
4. Challenge: V_{DD} Scalability

III. Measurement summary and Comparisons

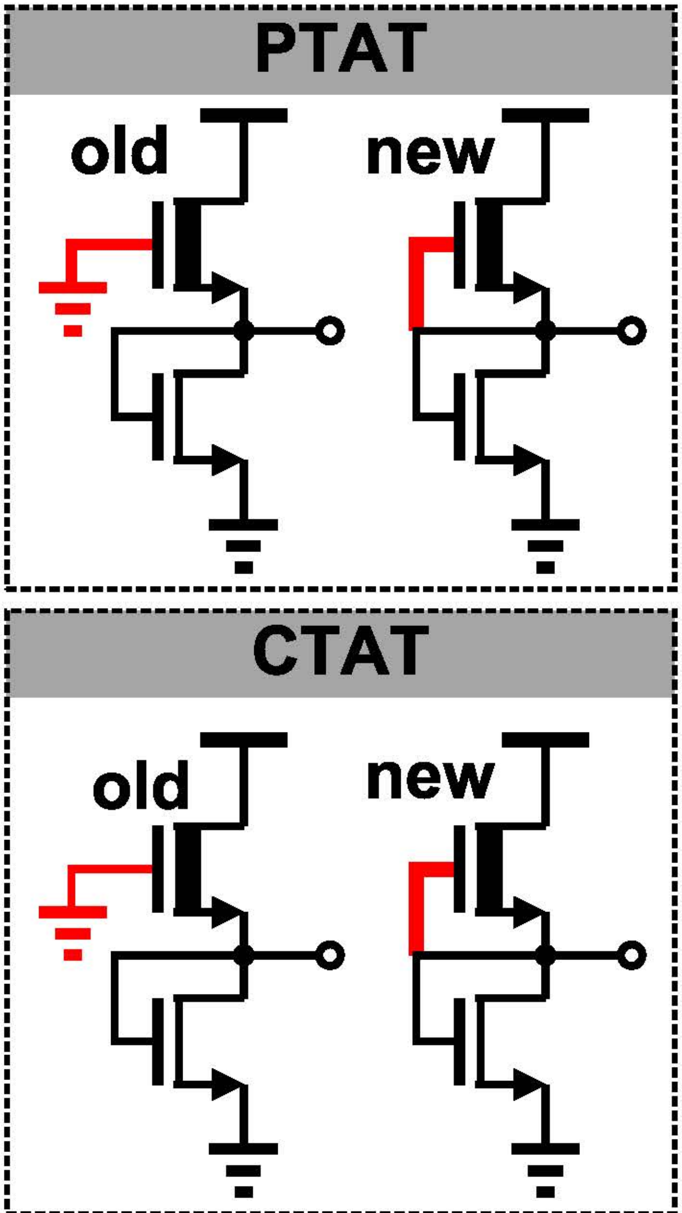
IV. Conclusion

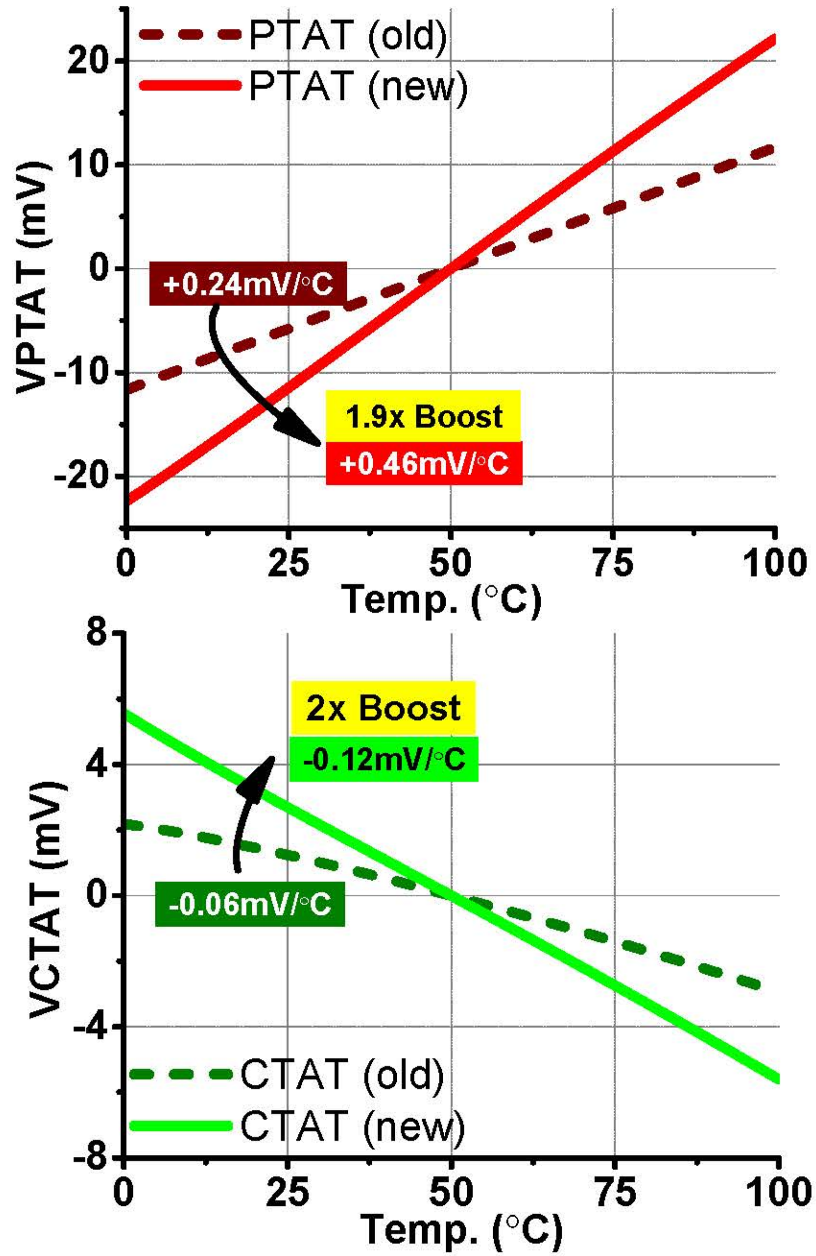
Enlarge Temp. Sensitivity with Up-Sizing



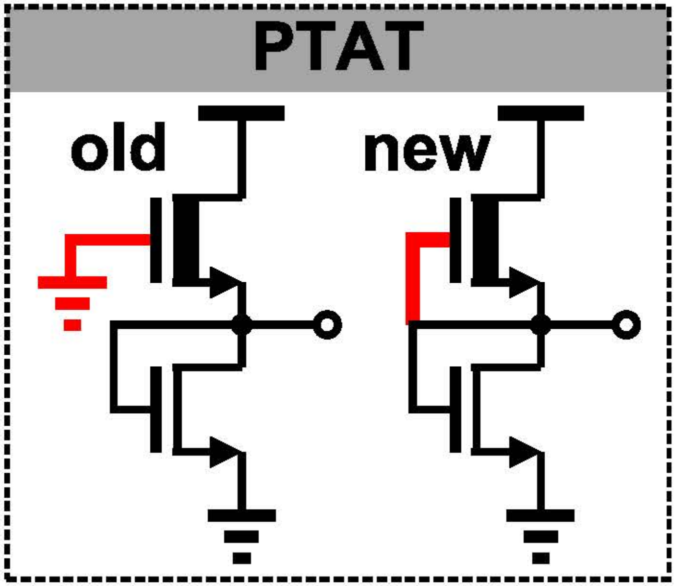
- Sizing ratio can modulate the slope
- **Too much area penalty!**

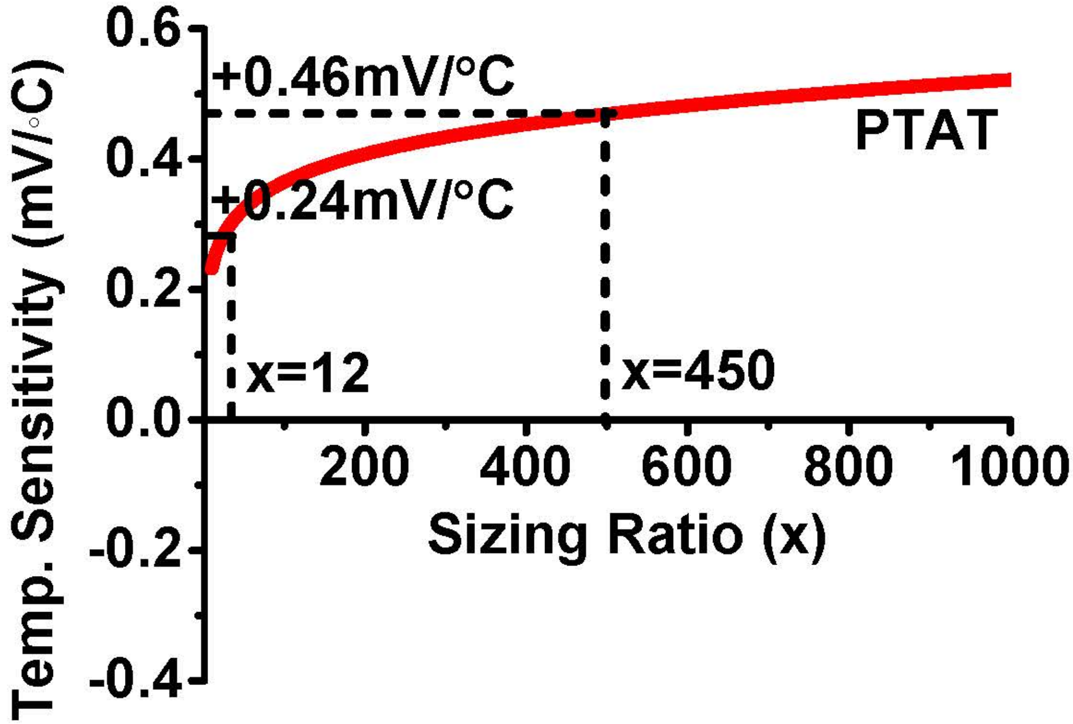
Gate Connection





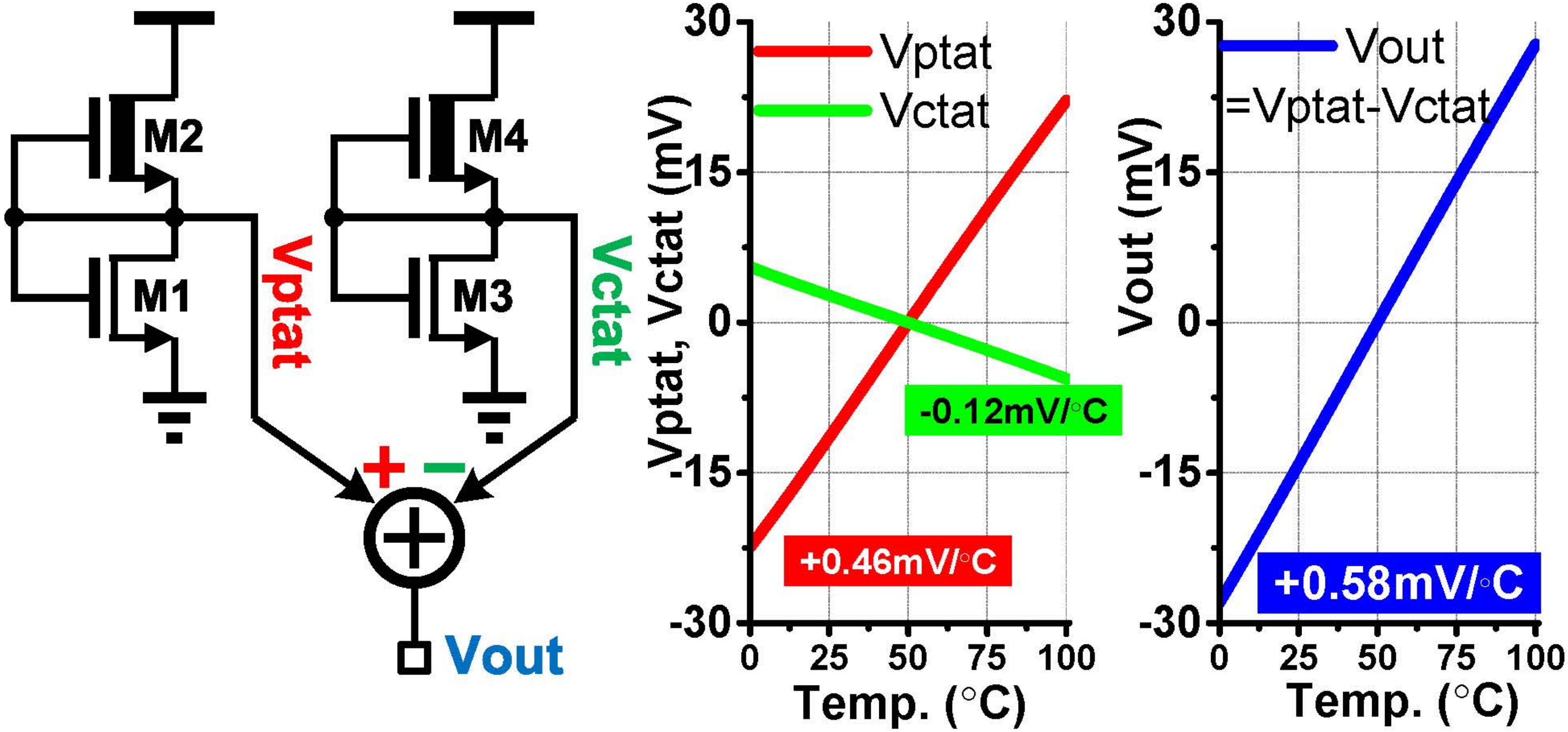
Example of Boost Temp. Sensitivity





- Sizing only: x=450
- Gate connection: x=12
- Same temp. sensitivity, 37.5x smaller area!

Differential Reading



- Differential reading increases the sensitivity
- <u>**More importantly**</u>, it can improve accuracy across temperature and process variations

Outline

I. Motivation and Design Overview

II. Design Approach

   1. Principles
   2. Challenge: Larger Temperature Sensitivity
   3. Challenge: Improve Accuracy
   4. Challenge: V_{DD} Scalability

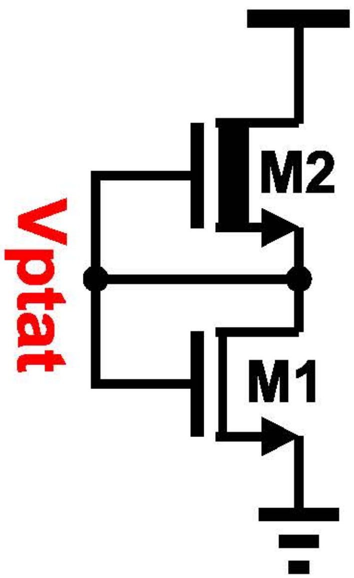
III. Measurement summary and Comparisons

IV. Conclusion

Nonlinearity of Single PTAT

Non-linear: Only PTAT used to estimate temperature

$$V_{ptat} = n_1\, ln\left(\frac{\mu_1}{\mu_2} \cdot \frac{C'_{ox1}}{C'_{ox2}} \cdot \frac{W_1 L_2}{W_2 L_1} \cdot \frac{n_1 - 1}{n_2 - 1}\right)\frac{k}{q} \cdot T + \left(V_{th1} - \frac{n_1}{n_2} V_{th2}\right)$$

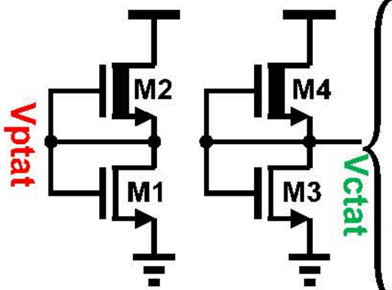


- M1 and M2 are different transistor types
  - Mobility:

$$\frac{\mu_1(T)}{\mu_2(T)} \neq const.\, across\ Temp.$$

→ Nonlinearity

Improve linearity with Differential Reading



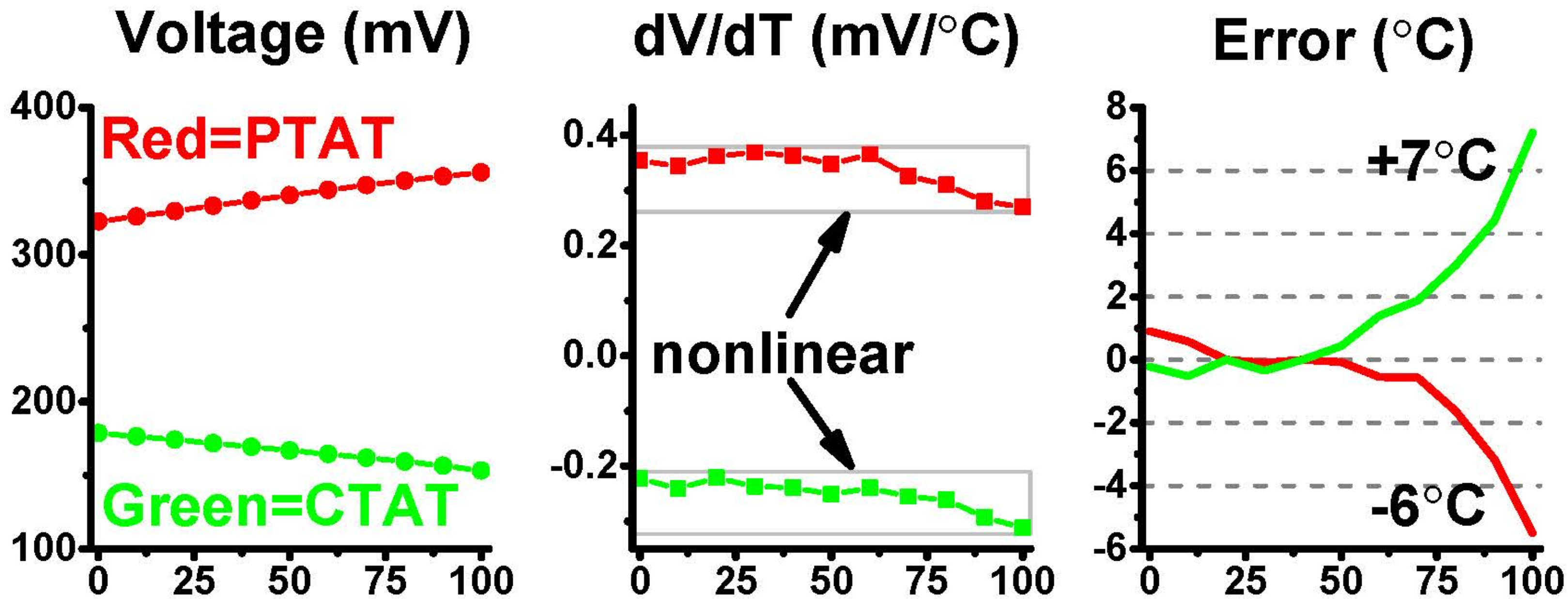
$$\begin{cases} V_{ptat} = n_1\, ln\left(\frac{\mu_1}{\mu_2}\cdot\frac{C'_{ox1}}{C'_{ox2}}\cdot\frac{W_1L_2}{W_2L_1}\cdot\frac{n_1-1}{n_2-1}\right)\frac{k}{q}\cdot T + \left(V_{th1} - \frac{n_1}{n_2}V_{th2}\right) \\ V_{ctat} = n_3\, ln\left(\frac{\mu_3}{\mu_4}\cdot\frac{C'_{ox3}}{C'_{ox4}}\cdot\frac{W_3L_4}{W_4L_3}\cdot\frac{n_3-1}{n_4-1}\right)\frac{k}{q}\cdot T + \left(V_{th3} - \frac{n_3}{n_4}V_{th4}\right) \end{cases}$$

- {M1,M3} =HVT nmos, {M2,M4} =native nmos
  - Sub-threshold factor: $n_1 \approx n_3$ $n_2 \approx n_4$
  - Mobility: $\mu_1 \approx \mu_3$ $\mu_2 \approx \mu_4$
  - Unit oxide capacitance: $C'_{ox1} \approx C'_{ox3}$ $C'_{ox2} \approx C'_{ox4}$

$$V_{out} = n_1\, ln\left(\frac{\cancel{\mu_1}}{\cancel{\mu_2}}\cdot\frac{\cancel{\mu_4}}{\cancel{\mu_3}}\cdot\frac{\cancel{C'_{ox1}}}{\cancel{C'_{ox2}}}\cdot\frac{\cancel{C'_{ox4}}}{\cancel{C'_{ox3}}}\cdot\frac{\cancel{n_1-1}}{\cancel{n_2-1}}\cdot\frac{\cancel{n_4-1}}{\cancel{n_3-1}}\cdot\frac{W_1L_2W_4L_3}{W_2L_1W_3L_4}\right)\frac{k}{q}\cdot T + \cdots$$

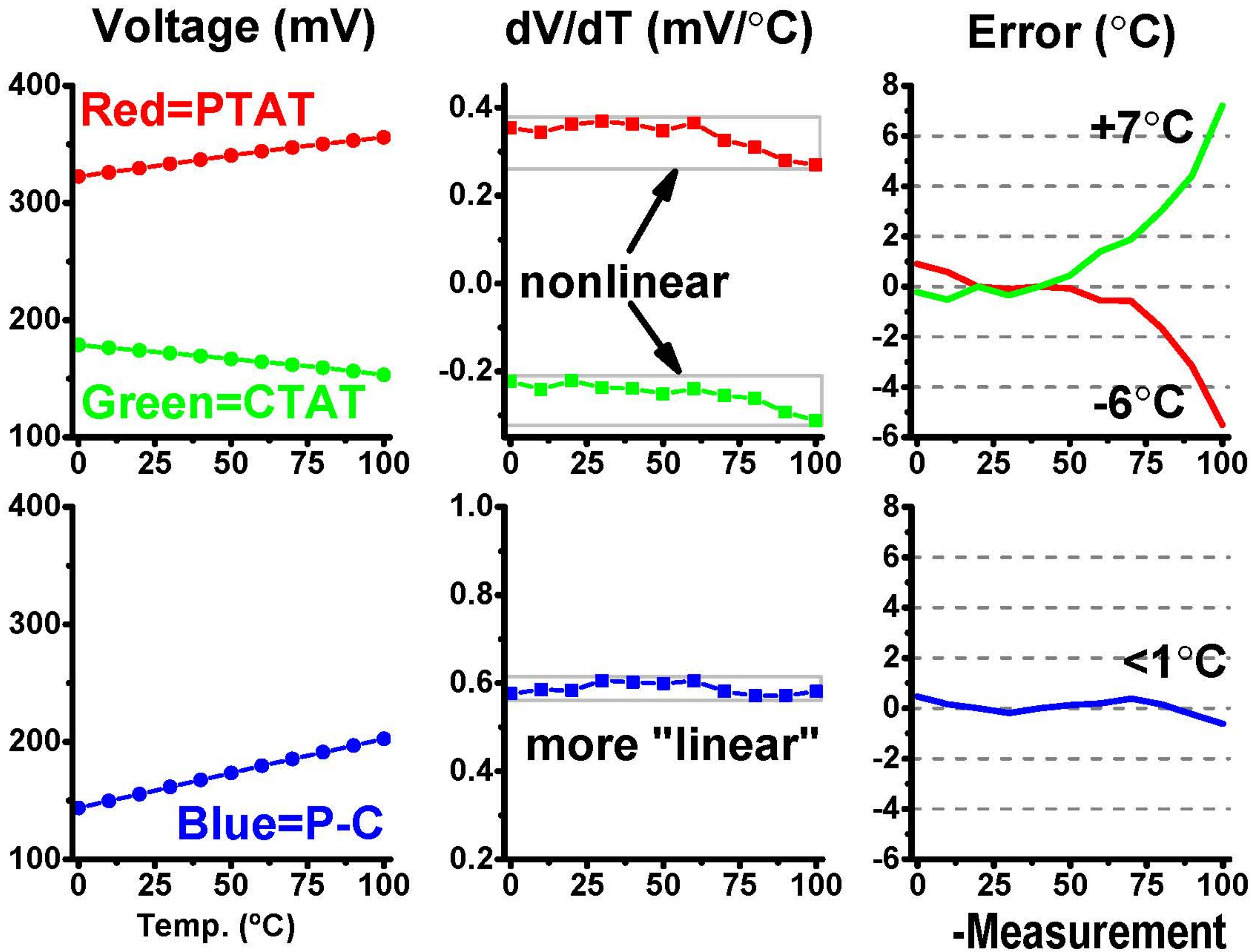
$$V_{out} = n_1\, ln\left(\frac{\boldsymbol{W_1L_2W_4L_3}}{\boldsymbol{W_2L_1W_3L_4}}\right)\frac{k}{q}\cdot T + \left(\Delta V_{th1,3} - \frac{n_1}{n_2}\Delta V_{th2,4}\right)$$

Nonlinearity of single PTAT or CTAT

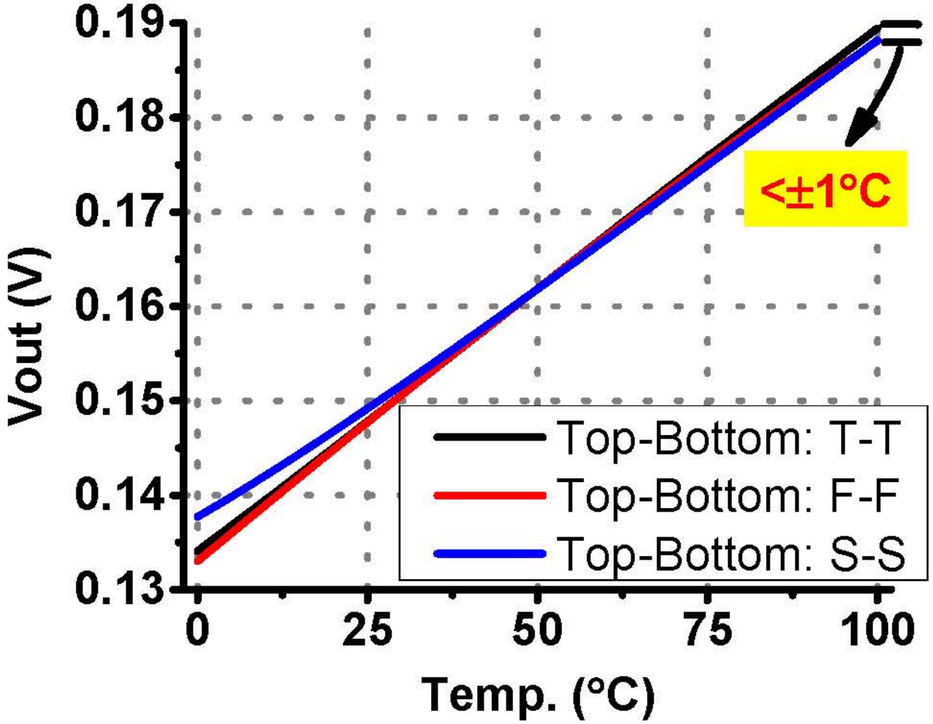


-Measurement

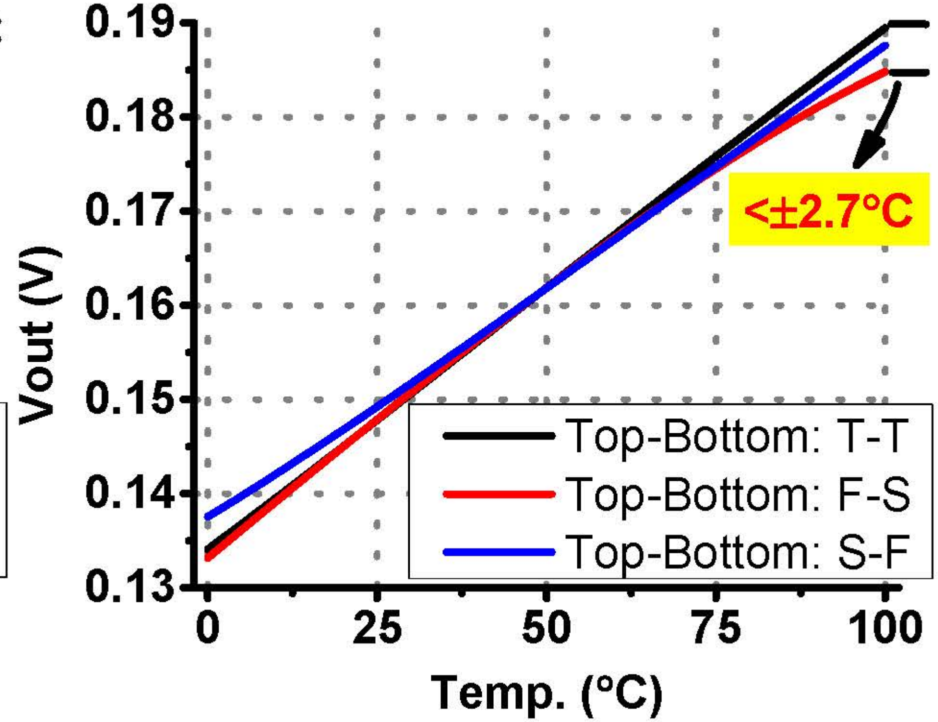
Improve linearity with Differential Reading



Accuracy Across Corners



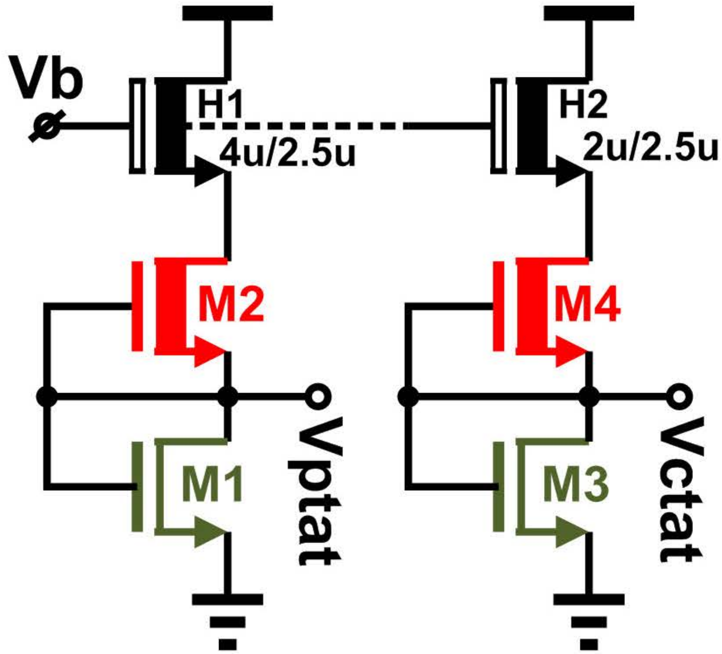
At the same corner

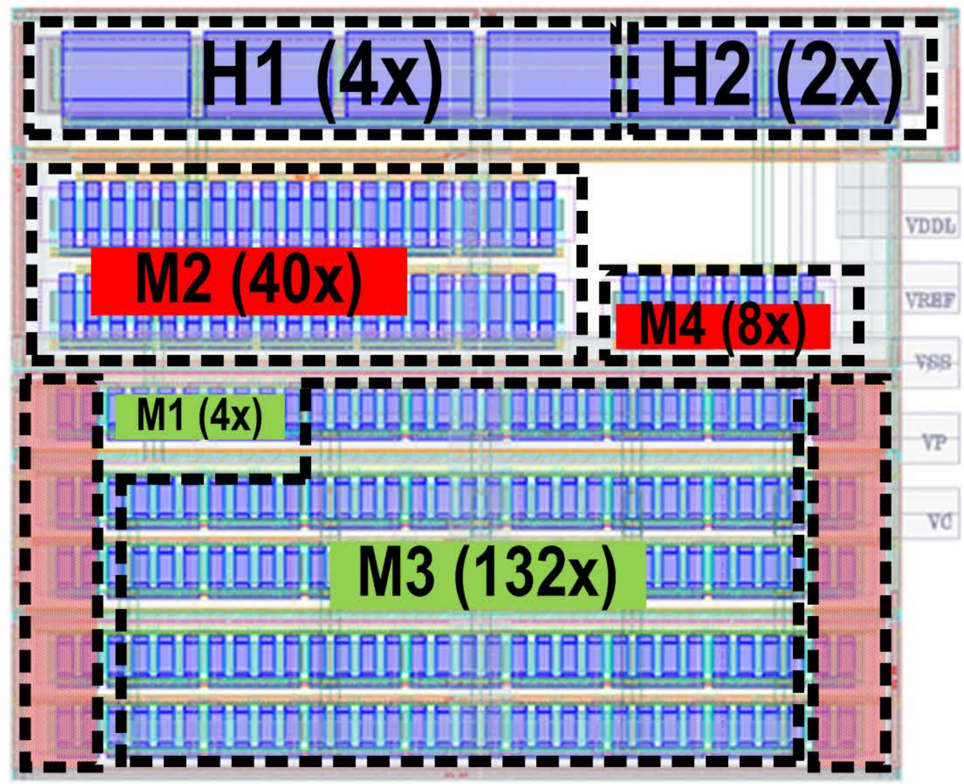


At the opposite corners

- Differential reading improves accuracy
  - T/B device at the same corner: <±1%
  - T/B device at the opposite corners: ±2.7%

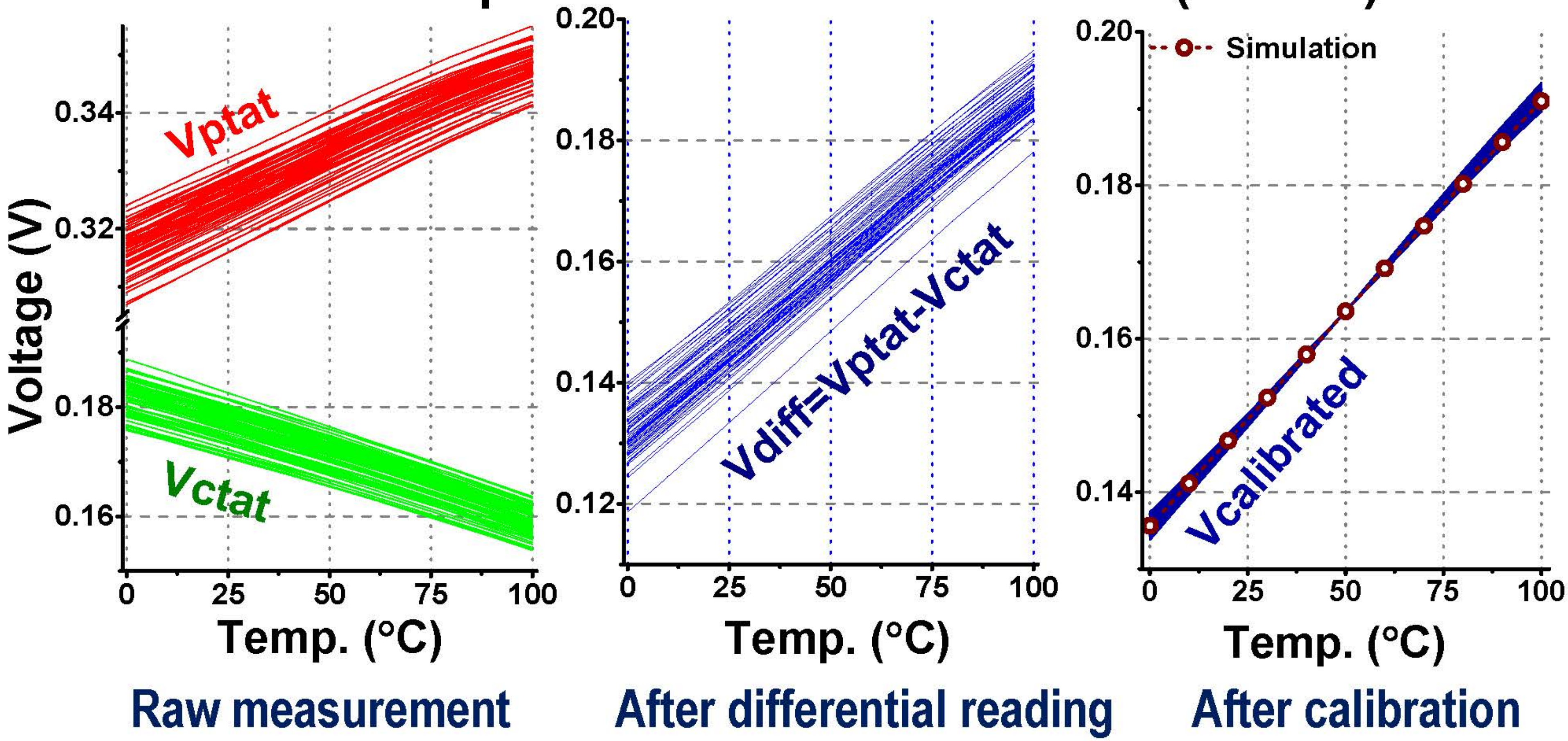
Careful Physical Design





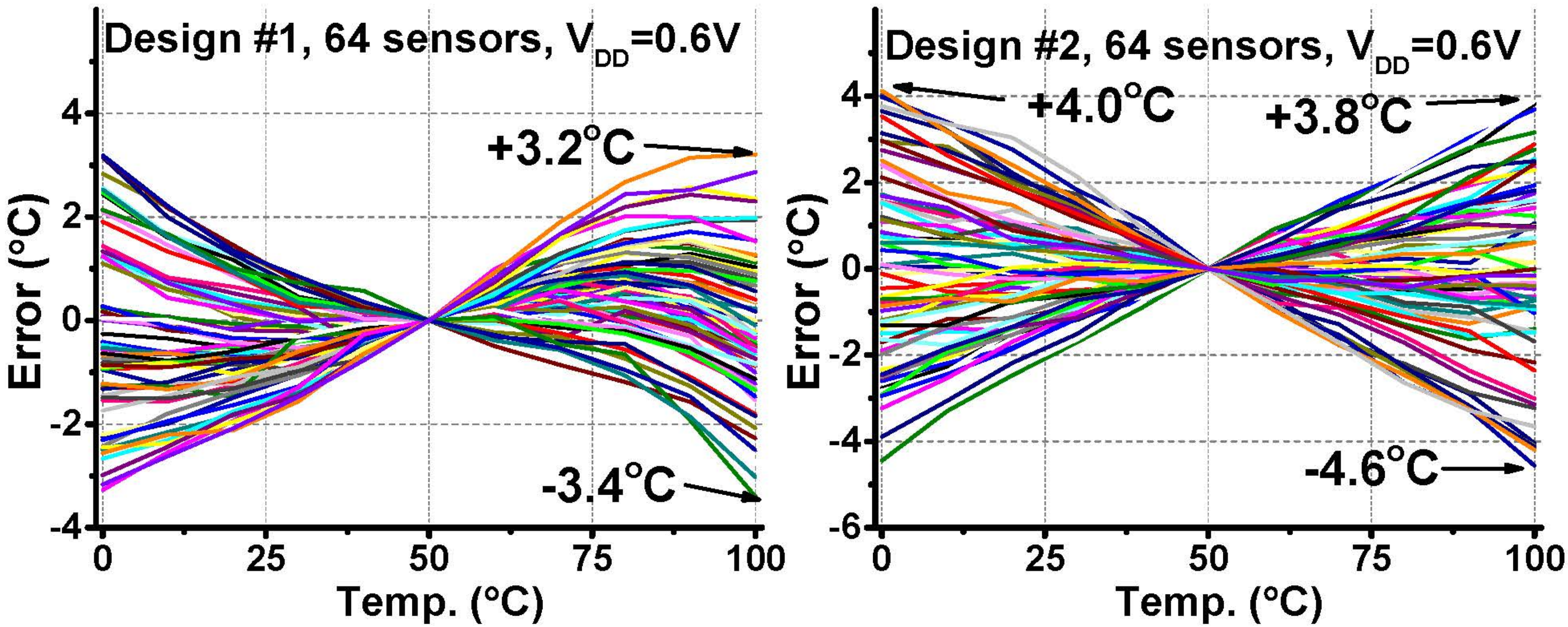
- Device: Same oxide thickness (M1,M2,M3,M4)
- Unit-device based layout
- Dummy transistors to reduce edge effect

One-temp. Point Calibration (OPC)



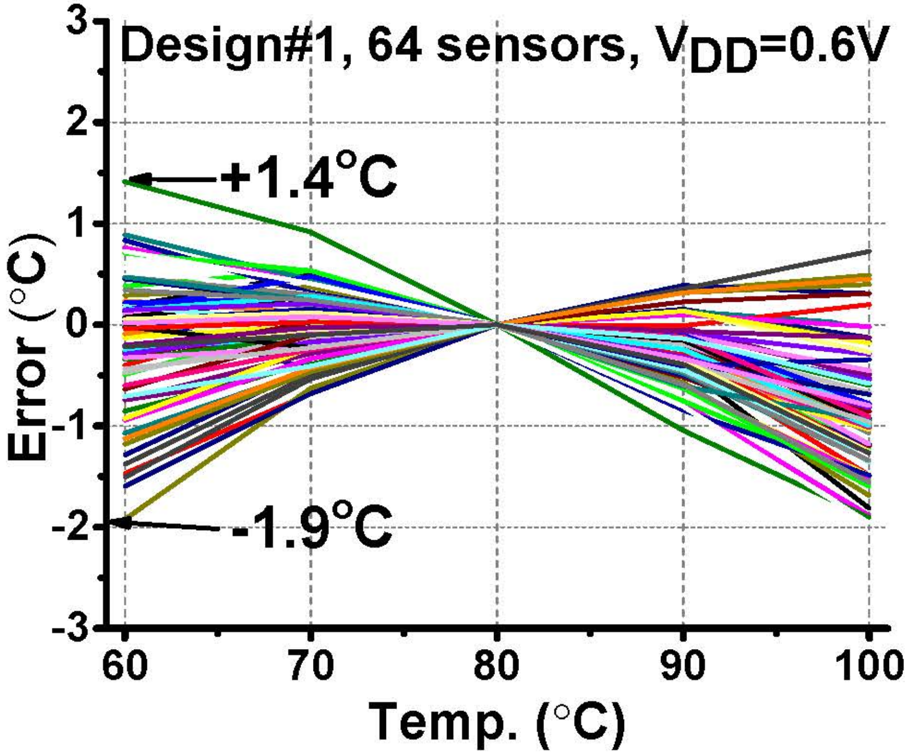
- Differential reading improves linearity
- OPC removes offset errors

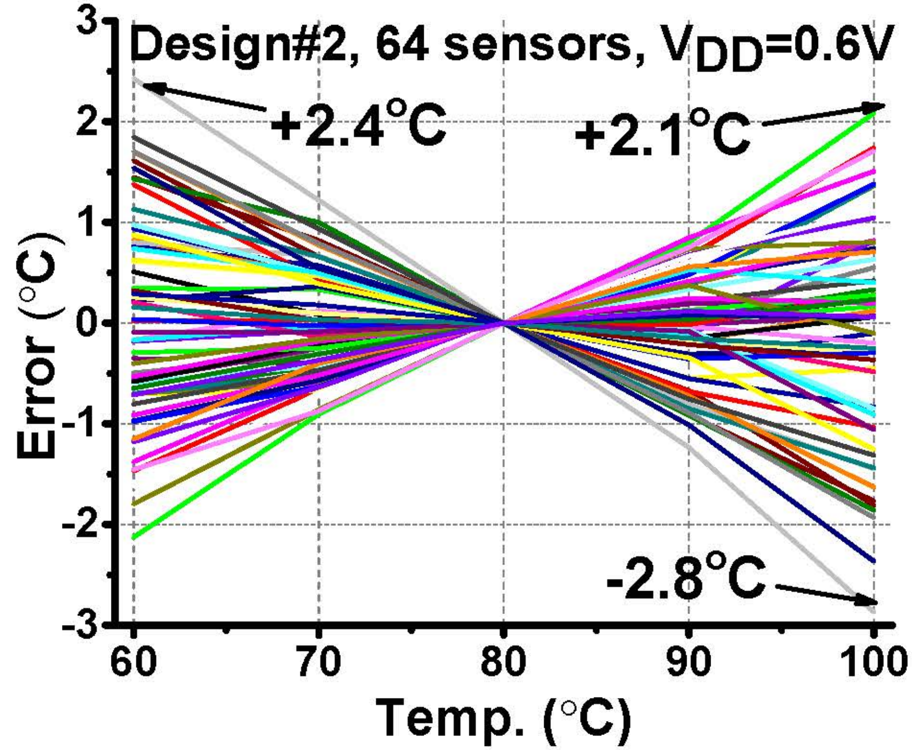
Accuracy over a Full Range



- Measurement from 64 sensors across 8 chips
- Range: $0^{o}C \sim 100^{o}C$, V_{DD}=0.6V, OPC@$50^{o}C$

Accuracy around a Throttle Range





- Measurement from 64 sensors across 8 chips
- Range: 60°C~100°C, V_{DD}=0.6V, OPC@80°C

Outline

I. Motivation and Design Overview

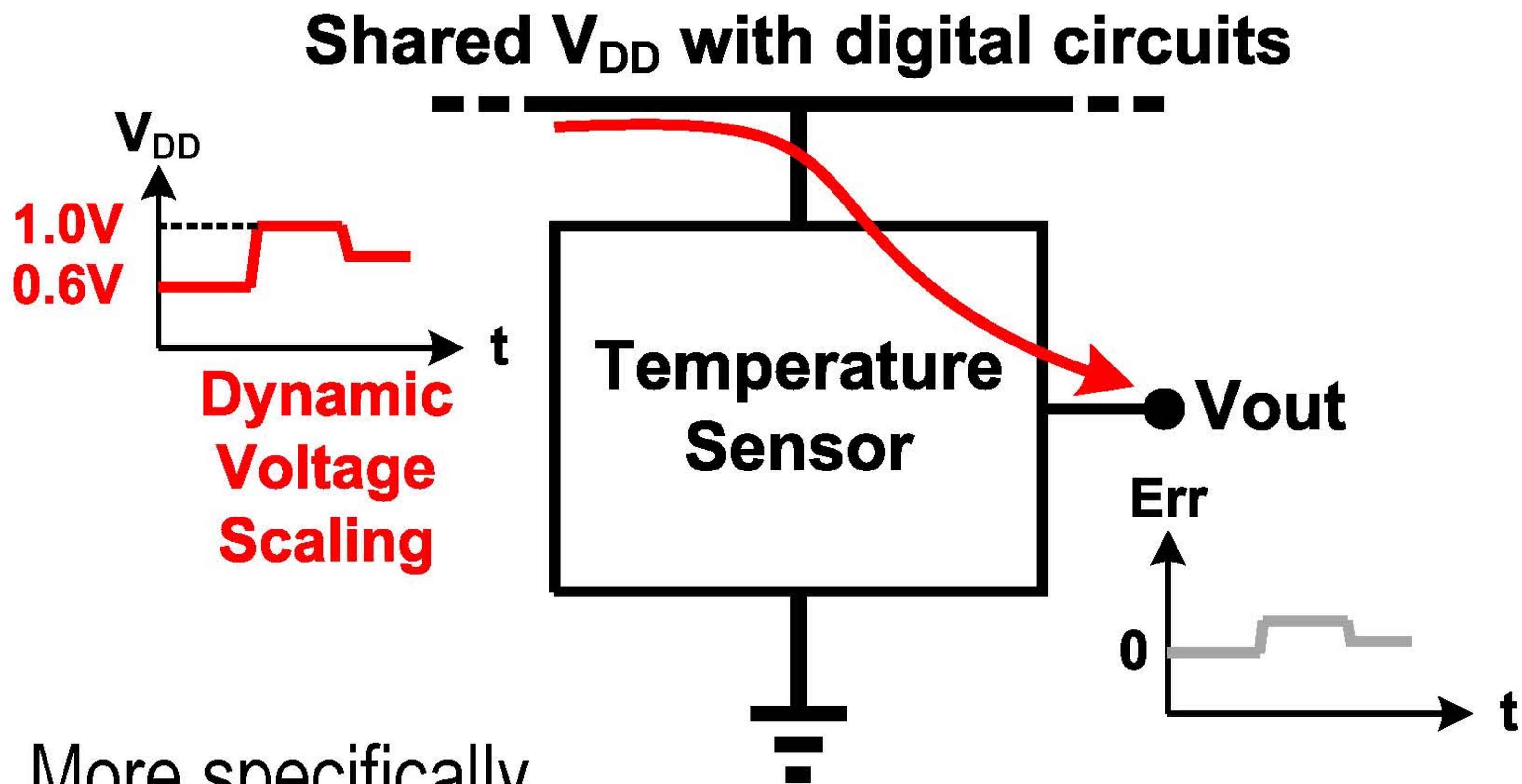
II. Design Approach

   1. Principles
   2. Challenge: Larger Temperature Sensitivity
   3. Challenge: Improve Accuracy
   4. Challenge: V_{DD} Scalability

III. Measurement summary and Comparisons

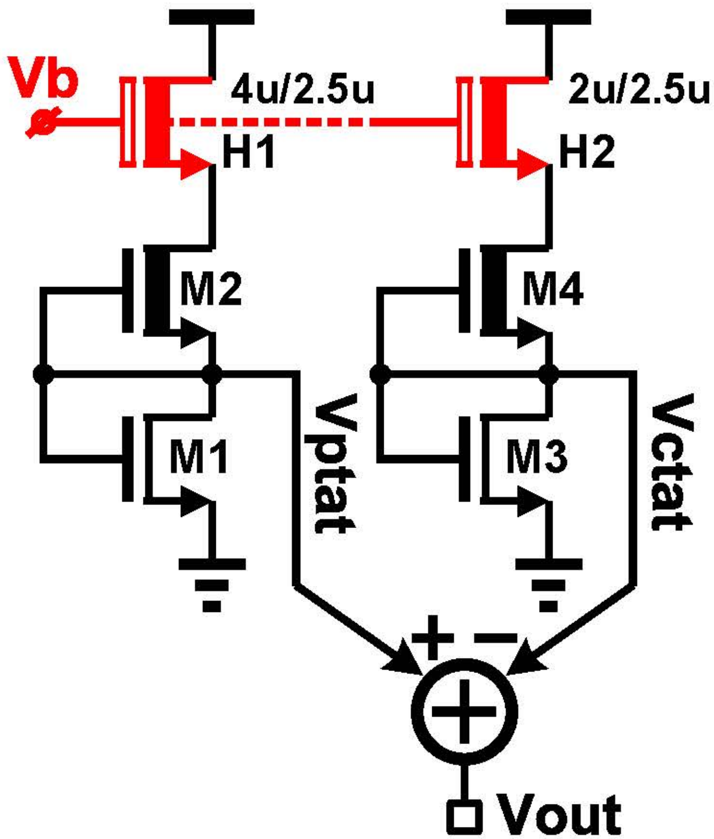
IV. Conclusion

V_{DD} Scalability and PSRR



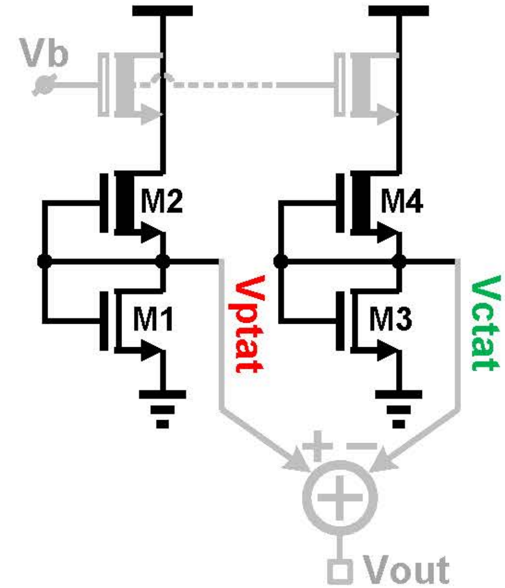
- More specifically…
  - Calibrate at V_{DD}=0.6V
  - Operate at V_{DD} =1.0V without extra calibrations?
- High DC-PSRR is critical

Improve PSRR with Cascode Devices

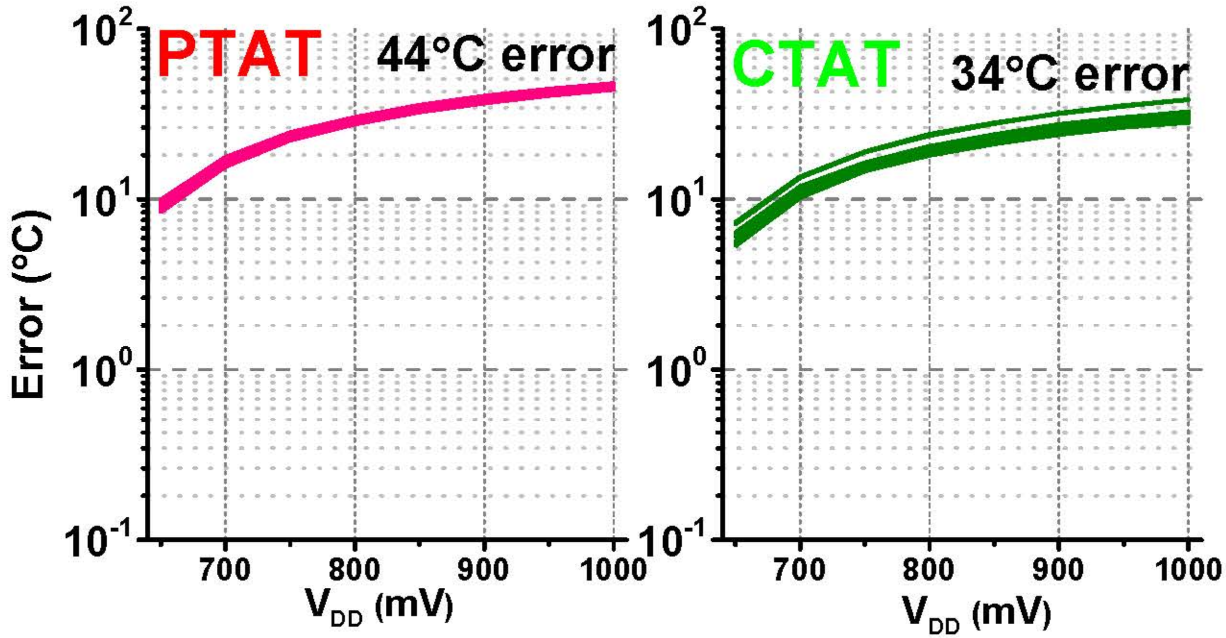


- Longer device (L↑)
  To maintain temperature sensitivity, W↑ → Area ↑
- Cascode device can improve PSRR

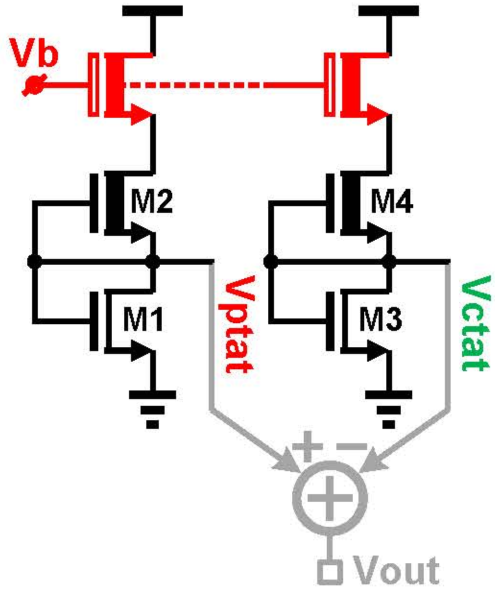
Large Error without Cascode Device



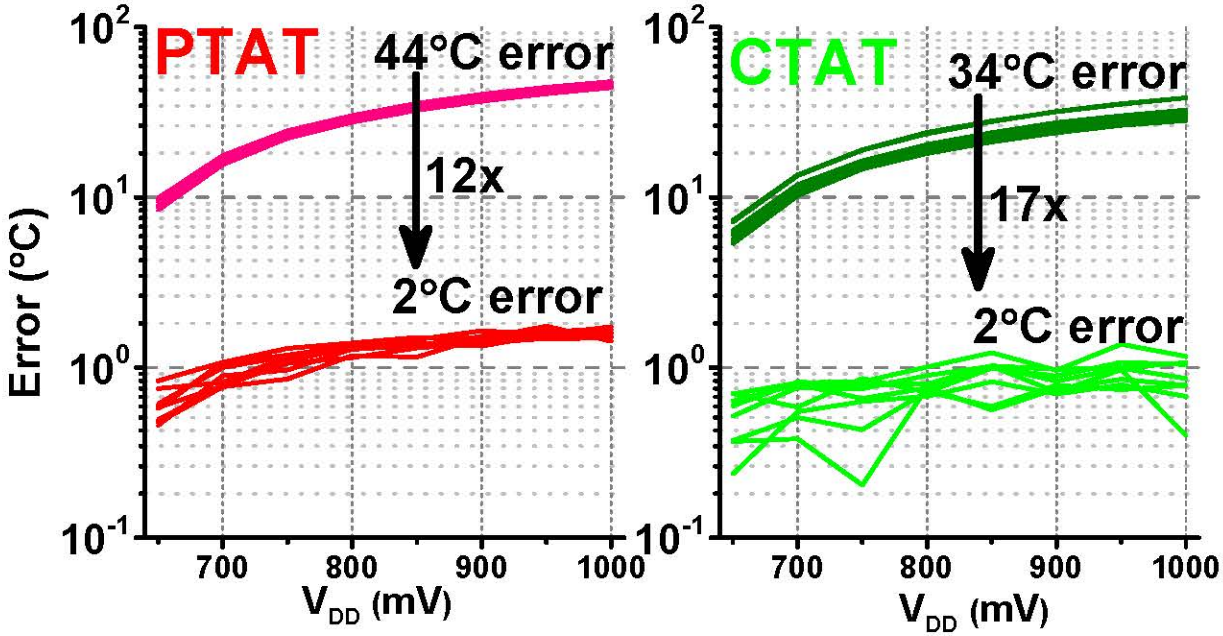
- PTAT or CTAT w.o. cascode
  Error: 44°C, 34°C



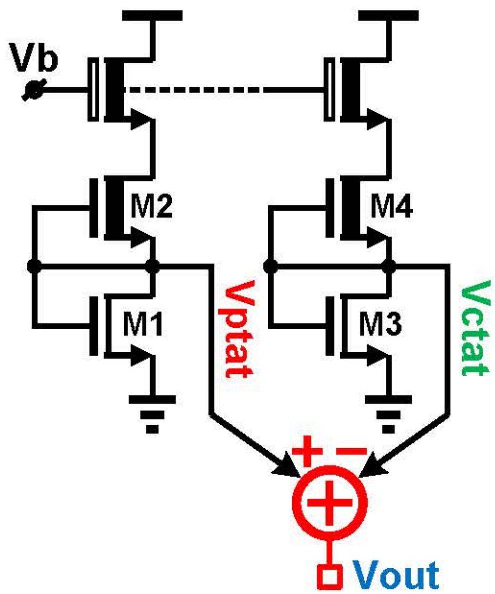
Error Reduced with Cascode Device



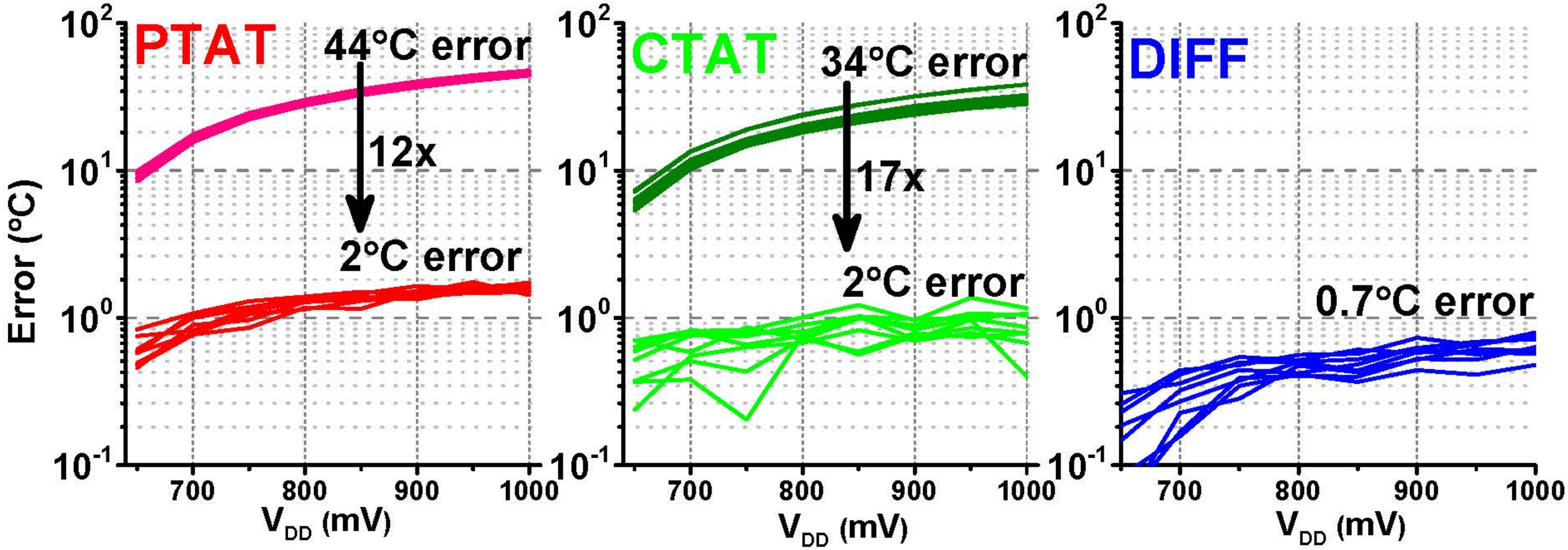
- PTAT or CTAT w.o. cascode
  Error: 44^{o}C, 34^{o}C
- PTAT or CTAT w. **cascode**
  Error: 2^{o}C, 2^{o}C



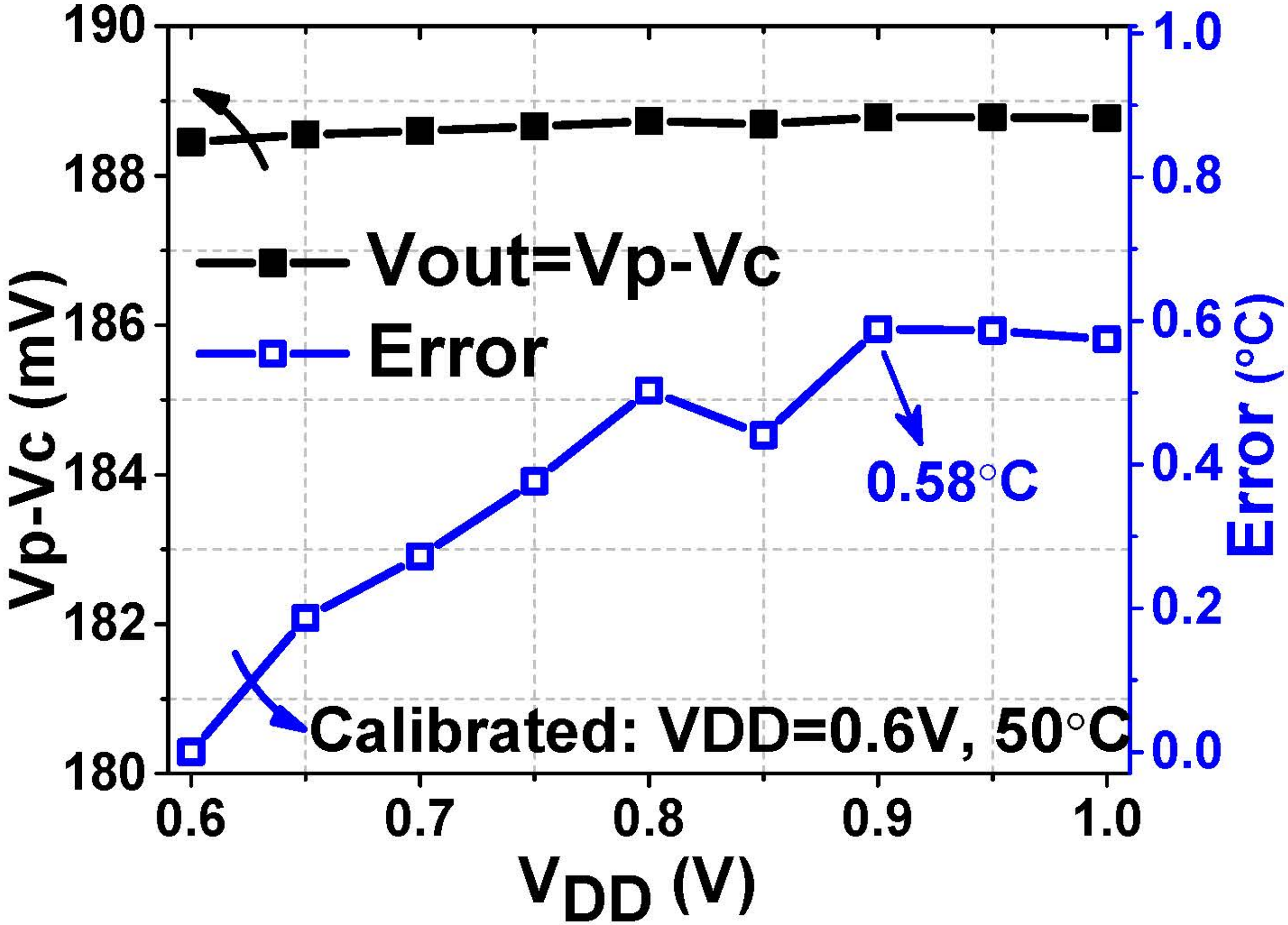
Differential Reading



- PTAT or CTAT w.o. cascode
  Error: 44°C, 34°C
- PTAT or CTAT w. cascode
  Error: 2°C, 2°C
- PTAT and CTAT **differential**
  Error: 0.7°C

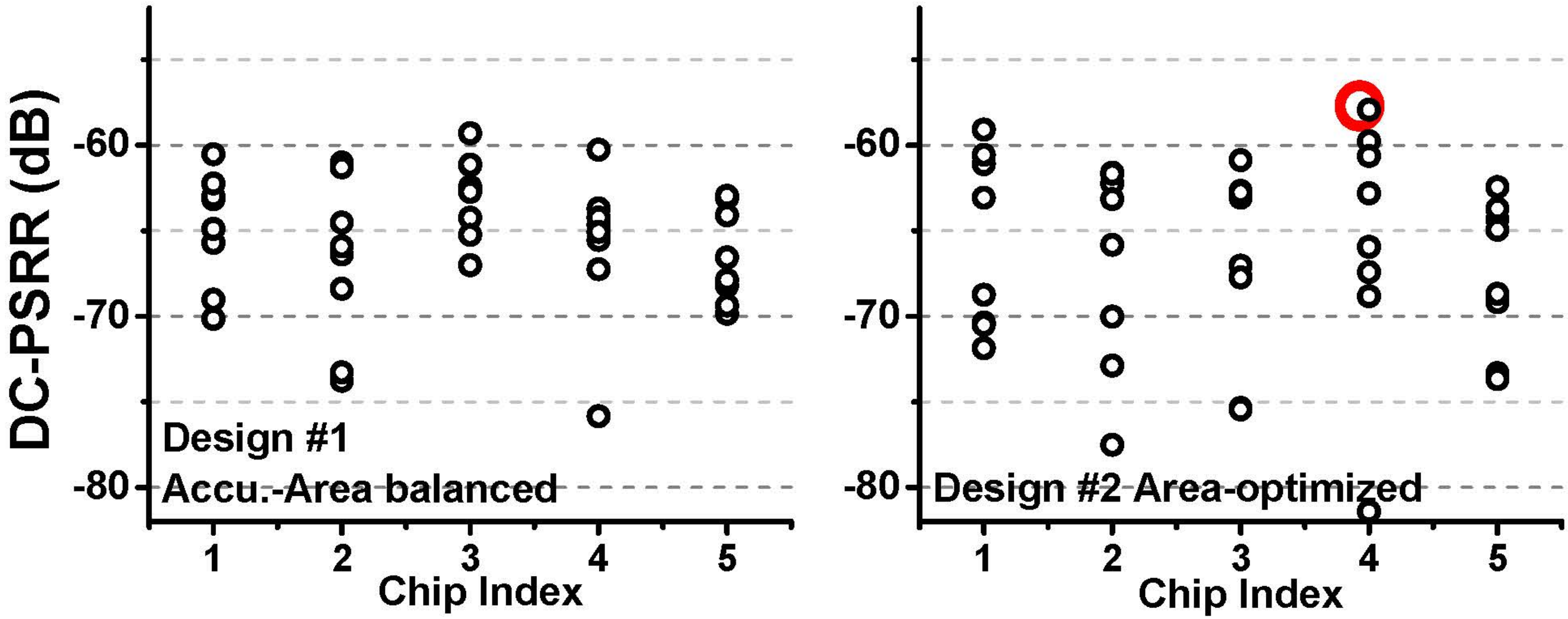


V_{DD} Scalability Measurement



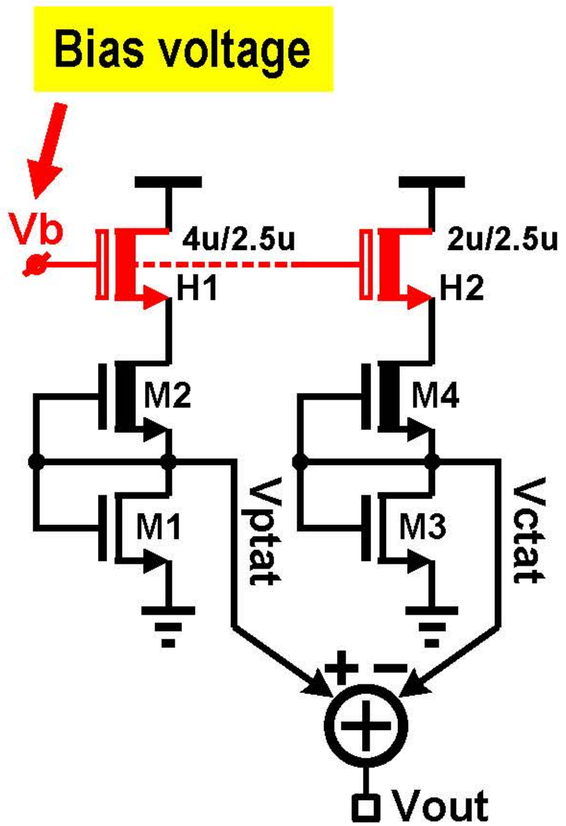
Error < 0.58°C at a typical chip

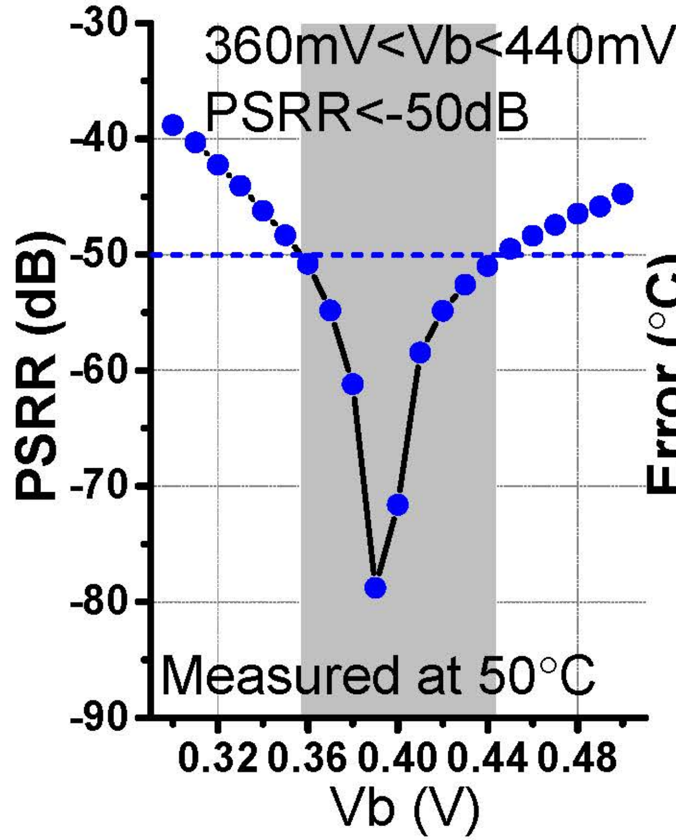
PSRR Measurements Across Chips

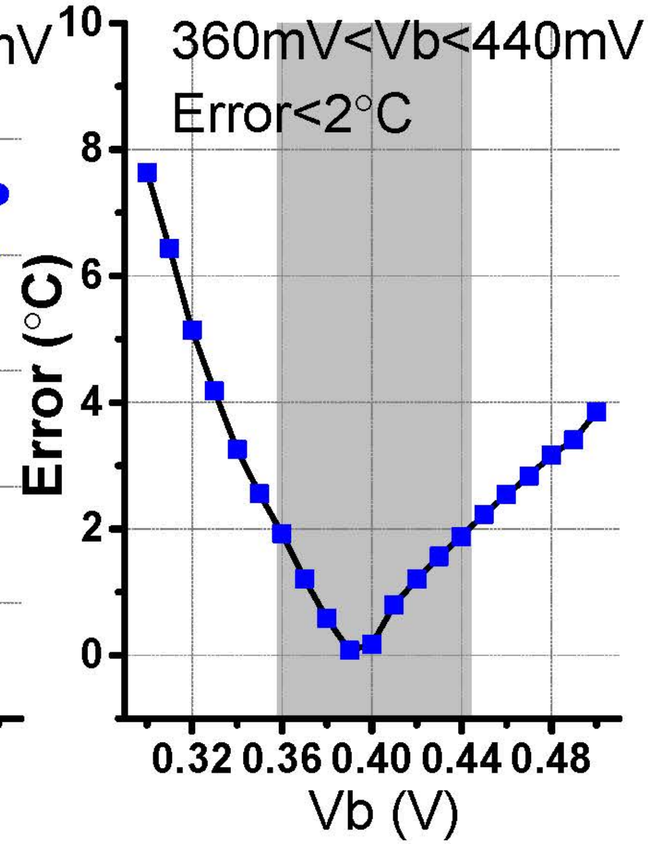


- 40 sensors from 5 chips
- Worst case:
  - -58dB PSRR
  - 0.73°C error with V_{DD}: 0.6V→ 1.0V

Requirement for the Cascode Bias Voltage





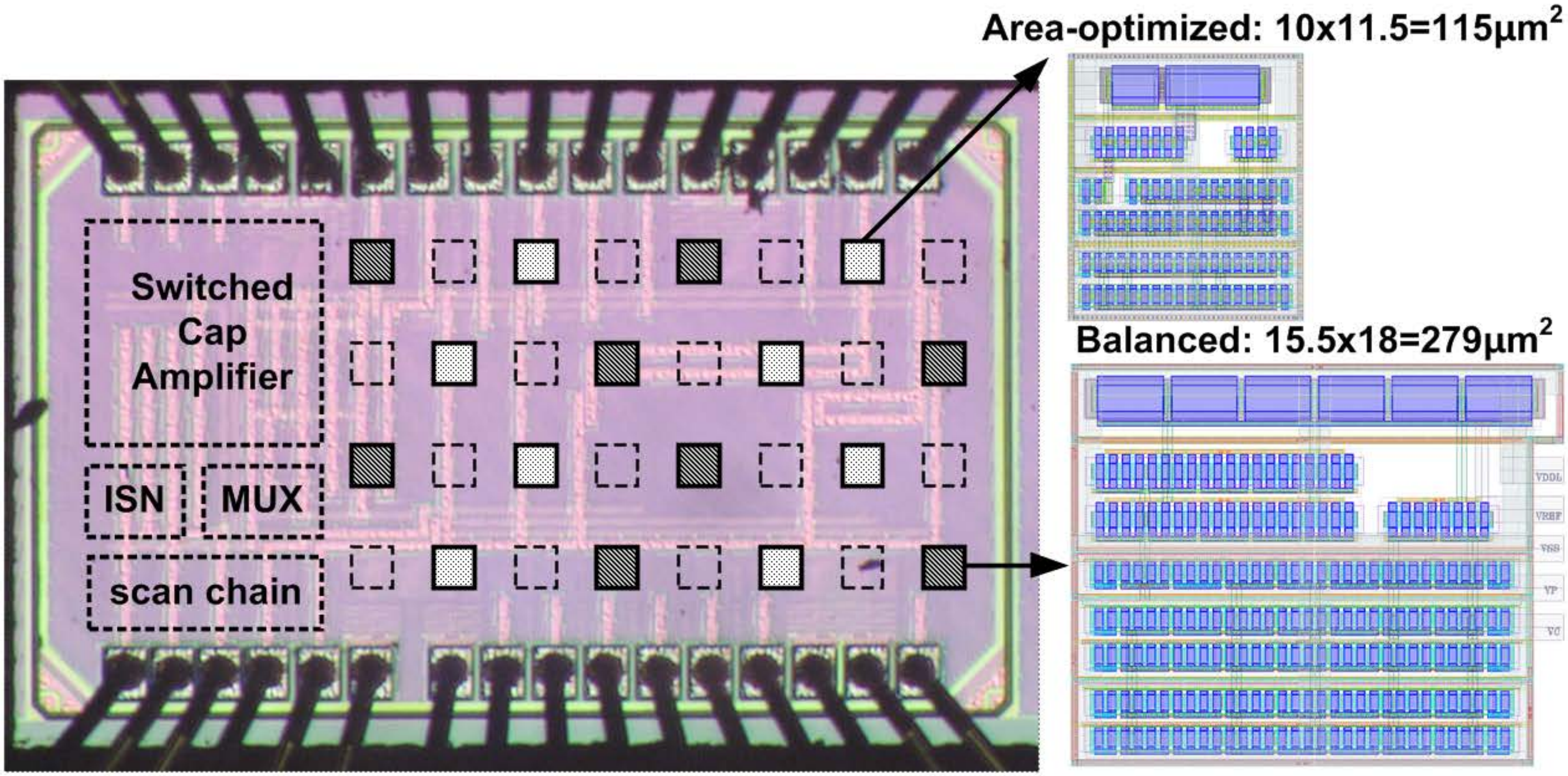


- Requirement of Vb: ±40mV guarantees <2°C error

Outline

I. Motivation and Design Overview
II. Design Approach
    1. Principles
    2. Challenge: Larger Temperature Sensitivity
    3. Challenge: Improve Accuracy
    4. Challenge: V_{DD} Scalability
III. Measurement summary and Comparisons
IV. Conclusion

Chip Die Photo

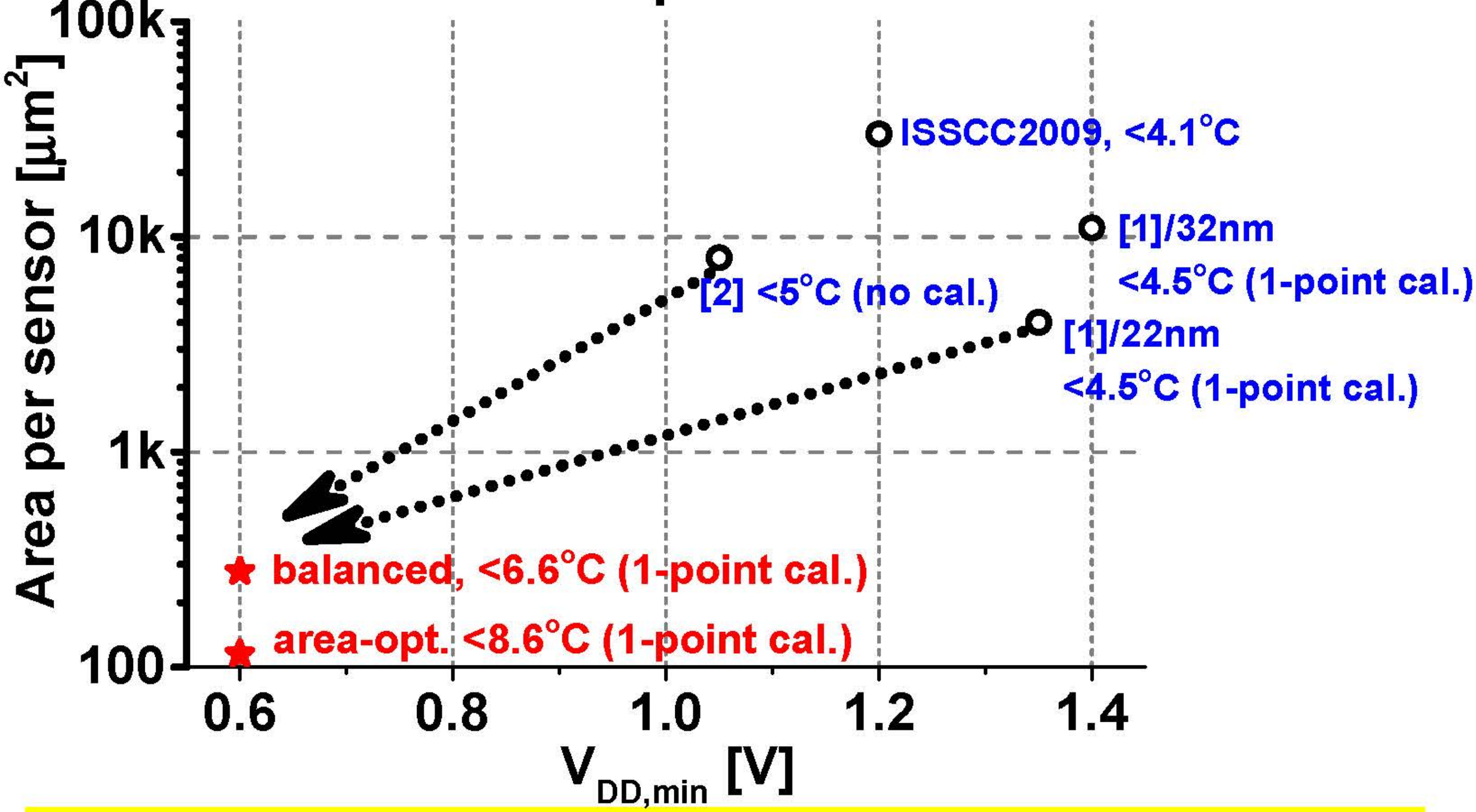


- 65nm CMOS
- Area = 0.77 X 1.2 mm^2

Measurement Summary

	Design #1 Area-accu. balanced	Design #2 Area-optimized
V_{DD} (V)	0.6~1.0	
V_{DD} induced Error (^{o}C/V)	1.2	0.8
Area (μm^2)	279	115
Power (μW)	<0.92	<0.21
Accuracy, OPC, full (^{o}C)	-3.4/+3.2	-4.6/+4.0
Accuracy, OPC, throttle (^{o}C)	-1.9/+1.4	-2.8/+2.4

Comparisons



- $V_{DD,min}$: 1.05V to 0.6V
- Area:
  - 4000μm² to 279μm², 14X reduction
  - 4000μm² to 115um², 34X reduction

Summary

- Temperature sensor is a key component in future VLSI systems
- Area reduction and V_{DD} scalability are paramount
- A new temperature sensor based on V_{th} is proposed, achieving:
  - V_{DD} scalability down to 0.6V
  - 14-34X area reduction

Acknowledgment

- Catalyst Foundation